目 录

1 对象策略 ····· 1-1
1.1 对象策略简介 ····· 1-1
1.1.1 对象策略规则的报文匹配条件 ····· 1-1
1.1.2 对象策略规则的编号 ····· 1-1
1.1.3 对象策略规则的匹配顺序 ····· 1-1
1.2 配置对象策略 ····· 1-1
1.2.1 配置任务简介 ····· 1-1
1.2.2 配置准备 ····· 1-2
1.2.3 创建对象策略 ····· 1-2
1.2.4 配置对象策略规则 ····· 1-3
1.2.5 安全域间实例应用对象策略 ····· 1-4
1.2.6 移动对象策略规则 ····· 1-5
1.2.7 使能对象策略加速功能 ····· 1-6
1.3 对象策略显示和维护 ····· 1-6
1.4 对象策略典型配置举例 ····· 1-7
1.4.1 对象策略规则配置举例 ····· 1-7

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。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 对象策略规则的报文匹配条件

一个对象策略中可以包含多条对象策略规则。对象策略规则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。

1.1.2 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。

1.1.3 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。

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
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：

- 创建 MDC（Multitenant Devices Context，多租户设备环境。请参见“虚拟化技术配置指导/MDC”）
- 配置时间段（请参见“ACL 和 QoS 配置指导/ACL”）
- 配置 IP 地址对象、IPv6 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

1. 创建IPv4 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**	-
进入MDC系统视图	**switchto mdc** *mdc-name*	仅对MDC必选
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，对象策略未配置任何描述信息

说明

有关 **switchto** 命令的详细介绍，请参见“虚拟化技术命令参考”中的“MDC”。

2. 创建IPv6 对象策略

表1-3 创建 IPv6 对象策略

操作	命令	说明
进入系统视图	**system-view**	-
进入MDC系统视图	**switchto mdc** *mdc-name*	仅对MDC必选
创建一个IPv6对象策略	**object-policy ipv6** *object-policy-name*	缺省情况下，不存在任何IPv6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

说明

有关 **switchto** 命令的详细介绍，请参见“虚拟化技术命令参考”中的“MDC”。

1.2.4 配置对象策略规则

1. 配置限制和指导

- 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。有关对象组的详细介绍请参见“安全配置指导”中的“对象组”。
- 在对象策略规则中引用应用和应用组时，请只引用 PBAR（Port Based Application Recognition，基于端口的应用层协议识别）类型的应用。若引用 NBAR（Network Based Application Recognition，基于内容特征的应用层协议识别）类型的应用，则此规则不会与任何报文匹配成功。有关 PBAR 和 NBAR 的详细介绍请参见“安全配置指导”中的“APR”。

2. 配置IPv4 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。
- 应用/应用组：用于与报文的应用 ID 进行匹配。

说明

有关对象组的详细介绍和配置，请参见“安全配置指导”中的“对象组”。

表1-4 配置对象策略规则

操作	命令	说明
进入系统视图	**system-view**	-
进入MDC系统视图	**switchto mdc** *mdc-name*	仅对MDC必选
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**| **inspect** *app-profile-name* } [[**source-ip** { *object-group-name* | **any** }] [**destination-ip** { *object-group-name* | **any** }] [**service** { *object-group-name* | **any** }] [**vrf** *vrf-name*] [**application** *application-name*] [**app-group** *app-group-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，规则未配置任何描述信息
（可选）为对象策略规则附加过滤条件	**rule** *rule-id* **append** { **application** *application-name* | **app-group** *app-group-name* | **destination-ip** *object-group-name* | **service** *object-group-name* | **source-ip** *object-group-name* }	缺省情况下，不存在规则的附加条件

3. 配置IPv6 对象策略规则

IPv6 对象策略规则可以指定引用的对象组，包括以下几种：

- 源 IPv6 地址对象组：用于与报文的源 IPv6 地址进行匹配。
- 目的 IPv6 地址对象组：用于与报文的目的 IPv6 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。
- 应用/应用组：用于与报文的应用 ID 进行匹配。

说明

有关对象组的详细介绍和配置，请参见“安全配置指导”中的“对象组”。

表1-5 配置对象策略规则

操作	命令	说明
进入系统视图	**system-view**	-
进入MDC系统视图	**switchto mdc** *mdc-name*	仅对MDC必选
创建IPv6对象策略，并进入其视图	**object-policy ipv6** *object-policy-name*	-
配置对象策略规则	**rule** [*rule-id*] { **drop** | **pass**| **inspect** *app-profile-name* } [[**source-ip** { *object-group-name* | **any** }] [**destination-ip** { *object-group-name* | **any** }] [**service** { *object-group-name* | **any** }] [**vrf** *vrf-name*] [**application** *application-name*] [**app-group** *app-group-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，规则未配置任何描述信息
（可选）为对象策略规则附加过滤条件	**rule** *rule-id* **append** { **application** *application-name* | **app-group** *app-group-name* | **destination-ip** *object-group-name* | **service** *object-group-name* | **source-ip** *object-group-name* }	缺省情况下，不存在规则的附加条件

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对象策略和一个IPv6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。

在安全域间实例应用对象策略前需配置 **zone-pair security** 命令创建安全域，关于安全域的详细介绍，请参见“基础配置命令参考”中的“安全域”。

表1-6 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**	-
进入MDC系统视图		**switchto mdc** *mdc-name*	仅对MDC必选
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
退回系统视图		**quit**	-
创建安全域间实例，并进入安全域间实例视图		**zone-pair security source** *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	应用IPv4对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内未应用任何对象策略规则
	应用IPv6对象策略	**object-policy apply ipv6** *object-policy-name*	

说明

有关 **switchto** 和 **zone-pair security** 命令的详细介绍，请分别参见“虚拟化技术命令参考” 中的“MDC”和“基础配置命令参考”中的“安全域”。

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1-7 移动对象策略规则

操作		命令	说明
进入系统视图		**system-view**	-
进入MDC系统视图		**switchto mdc** *mdc-name*	仅对MDC必选
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*	-
	进入IPv6对象策略视图	**object-policy ipv6** *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1-8 使能对象策略加速功能

操作		命令	说明
进入系统视图		**system-view**	-
进入MDC系统视图		**switchto mdc** *mdc-name*	仅对MDC必选
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*	-
	进入IPv6对象策略视图	**object-policy ipv6** *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

说明

有关 **switchto** 命令的详细介绍，请参见“虚拟化技术命令参考”中的“MDC”。

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1-9 对象策略显示和维护

配置	命令
显示对象策略的加速状态（独立运行模式）	**display object-policy accelerate** { **summary** { **ip** | **ipv6** } | **verbose** { **ip** *object-policy-name* | **ipv6** *object-policy-name* } **slot** *slot-number* }
显示对象策略的加速状态（IRF模式）	**display object-policy accelerate** { **summary** { **ip** | **ipv6** } | **verbose** { **ip** *object-policy-name* | **ipv6** *object-policy-name* } **chassis** *chassis-number* **slot** *slot-number* }
显示IPv4对象策略的配置信息	**display object-policy ip** [*object-policy-name*]
显示IPv6对象策略的配置信息	**display object-policy ipv6** [*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*]

配置	命令
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** | **ipv6**]

1.4 对象策略典型配置举例

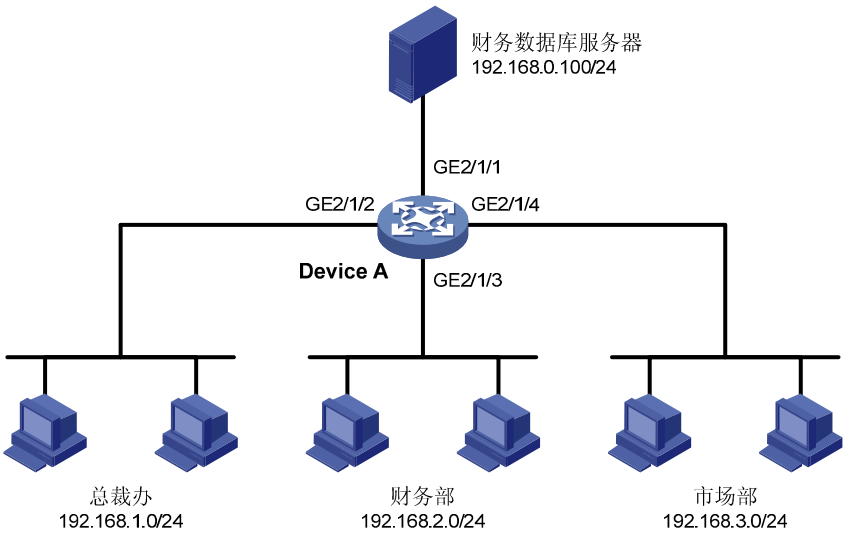
1.4.1 对象策略规则配置举例

1. 组网需求

- 某公司内的各部门之间通过 Device A 实现互连，该公司的工作时间为每周工作日的 8 点到 18 点。
- 通过配置对象策略规则，允许总裁办在任意时间、财务部在工作时间通过 HTTP 协议访问财务数据库服务器的 Web 服务，禁止其它部门在任何时间、财务部在非工作时间通过 HTTP 协议访问该服务器的 Web 服务。

2. 组网图

图1-1 对象策略配置组网图



3. 配置步骤

(1) 配置时间段

创建名为 work 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<DeviceA> system-view
[DeviceA] time-range work 08:00 to 18:00 working-day
```

(2) 配置安全域

创建名为 president 的安全域，并将接口 GigabitEthernet2/1/2 加入该安全域中。

```
[DeviceA] security-zone name president
[DeviceA-security-zone-president] import interface gigabitethernet 2/1/2
[DeviceA-security-zone-president] quit
```

创建名为 finance 的安全域，并将接口 GigabitEthernet2/1/3 加入该安全域中。

```
[DeviceA] security-zone name finance
[DeviceA-security-zone-finance] import interface gigabitethernet 2/1/3
[DeviceA-security-zone-finance] quit
```

创建名为 market 的安全域，并将接口 GigabitEthernet2/1/4 加入该安全域中。

```
[DeviceA] security-zone name market
[DeviceA-security-zone-market] import interface gigabitethernet 2/1/4
[DeviceA-security-zone-market] quit
```

创建名为 database 的安全域，并将接口 GigabitEthernet2/1/1 加入该安全域中。

```
[DeviceA] security-zone name database
[DeviceA-security-zone-database] import interface gigabitethernet 2/1/1
[DeviceA-security-zone-database] quit
```

(3) 配置对象

创建名为 president 的 IP 地址对象组，并定义其子网地址为 192.168.1.0/24。

```
[DeviceA] object-group ip address president
[DeviceA-obj-grp-ip-president] network subnet 192.168.1.0 24
[DeviceA-obj-grp-ip-president] quit
```

创建名为 finance 的 IP 地址对象组，并定义其子网地址为 192.168.2.0/24。

```
[DeviceA] object-group ip address finance
[DeviceA-obj-grp-ip-finance] network subnet 192.168.2.0 24
[DeviceA-obj-grp-ip-finance] quit
```

创建名为 market 的 IP 地址对象组，并定义其子网地址为 192.168.3.0/24。

```
[DeviceA] object-group ip address market
[DeviceA-obj-grp-ip-market] network subnet 192.168.3.0 24
[DeviceA-obj-grp-ip-market] quit
```

创建名为 database 的 IP 地址对象组，并定义其子网地址为 192.168.0.0/24。

```
[DeviceA] object-group ip address database
[DeviceA-obj-grp-ip-database] network subnet 192.168.0.0 24
[DeviceA-obj-grp-ip-database] quit
```

创建名为 web 的服务对象组，并定义其支持的服务为 HTTP。

```
[DeviceA] object-group service web
[DeviceA-obj-grp-service-web] service 6 destination eq 80
[DeviceA-obj-grp-service-web] quit
```

(4) 配置对象策略及规则

制订允许总裁办在任意时间通过 HTTP 协议访问财务数据库服务器的对象策略及规则。

```
[DeviceA] object-policy ip president-database
[DeviceA-object-policy-ip-president-database] rule pass source-ip president destination-ip
database service web
[DeviceA-object-policy-ip-president-database] quit
```

制订只允许财务部在工作时间通过 HTTP 协议访问财务数据库服务器的对象策略及规则。

```
[DeviceA] object-policy ip finance-database
[DeviceA-object-policy-ip-finance-database] rule pass source-ip finance destination-ip
database service web time-range work
[DeviceA-object-policy-ip-finance-database] quit
```

制订禁止市场部在任何时间通过 HTTP 协议访问财务数据库服务器的对象策略及规则。

```
[DeviceA] object-policy ip market-database
[DeviceA-object-policy-ip-market-database] rule drop source-ip market destination-ip database service web
[DeviceA-object-policy-ip-market-database] quit
```

(5) 配置安全域间实例并应用对象策略

创建源安全域 president 到目的安全域 database 的安全域间实例，并应用允许总裁办在任意时间通过 HTTP 协议访问财务数据库服务器的对象策略。

```
[DeviceA] zone-pair security source president destination database
[DeviceA-zone-pair-security-president-database] object-policy apply ip president-database
[DeviceA-zone-pair-security-president-database] quit
```

创建源安全域 finance 到目的安全域 database 的安全域间实例，并应用只允许财务部在工作时间通过 HTTP 协议访问财务数据库服务器的对象策略。

```
[DeviceA] zone-pair security source finance destination database
[DeviceA-zone-pair-security-finance-database] object-policy apply ip finance-database
[DeviceA-zone-pair-security-finance-database] quit
```

创建源安全域 market 到目的安全域 database 的安全域间实例，并应用禁止市场部在任何时间通过 HTTP 协议访问财务数据库服务器的对象策略。

```
[DeviceA] zone-pair security source market destination database
[DeviceA-zone-pair-security-market-database] object-policy apply ip market-database
[DeviceA-zone-pair-security-market-database] quit
```

4. 验证配置

配置完成后，在各部门的 PC 上可通过网络浏览器对财务数据库服务器的 Web 服务进行访问验证。