# 目 录

# 1 数据过滤

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

| 型号 | 特性 | 描述 |
| --- | --- | --- |
| F5010/F5020/F5030/F5030-6GW/F5040/F5060/F5080/F5000-M/F5000-S/F5000-C | 数据过滤 | 支持 |
| F1005/F1010/F1020/F1030/F1050/F1060/F1070/F1080/F1070-GM | | • F1005/F1010：不支持<br>• F1020/F1030/F1050/F1060/F1070/F1080/F1070-GM：支持 |
| F1000-AK108/AK109/AK110/AK115/AK120/AK125/AK130/AK135/AK140/AK145/AK150/AK155/AK160/AK165/AK170/AK175/AK180/AK185/AK710/AK711 | | • F1000-AK108/AK109/AK110/AK115/AK120/AK125/AK710：不支持<br>• F1000-AK130/AK135/AK140/AK145/AK150/AK155/AK160/AK165/AK170/AK175/AK180/AK185/AK711：支持 |
| F1000-GM-AK370/F1000-GM-AK380 | | 支持 |
| LSU3FWCEA0/LSUM1FWCEAB0/LSX1FWCEA1 | | 支持 |
| LSXM1FWDF1/LSUM1FWDEC0/IM-NGFWX-IV/LSQM1FWDSC0/LSWM1FWD0/LSPM6FWD | | 支持 |

## 1.1 数据过滤简介

数据过滤是一种对流经设备的报文的应用层信息进行过滤的安全防护机制。采用数据过滤功能可以有效防止内网机密信息泄露，禁止内网用户在 Internet 上浏览、发布和传播违规或违法信息。目前，数据过滤功能支持对基于以下应用层协议传输的应用层信息进行检测和过滤。

- HTTP（Hypertext Transfer Protocol，超文本传输协议）
- FTP（File Transfer Protocol，文件传输协议）
- SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）

### 1.1.1 基本概念

#### 1. 数据过滤特征

数据过滤特征是设备上定义的用于识别应层信息特征的字符串。

#### 2. 关键字组

关键字组用来对数据过滤特征进行统一组织和管理。一个关键字组中可以包含 32 个特征，且它们之间是或的关系。

#### 3. 数据过滤规则

数据过滤规则是报文应用层信息安全检测条件及处理动作的集合。在一个规则中可设置关键字组、报文方向、应用类型和动作（丢弃、放行、生成日志）。只有报文成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

### 1.1.2 数据过滤的实现原理

设备对报文进行数据过滤处理的整体流程如下：

(1) 如果策略（即安全策略或对象策略）引用了数据过滤业务，当设备收到 HTTP、FTP、SMTP 报文时，设备将对匹配了策略的报文进行数据过滤处理。有关安全策略的详细介绍请参见“安全配置指导”中的“安全策略”；有关对象策略规则的详细介绍请参见“安全配置指导”中的“对象策略”。

(2) 设备提取报文中的应用层信息与数据过滤规则进行匹配，并根据匹配结果对报文执行动作：

- 如果报文同时与多个规则匹配成功，则执行这些规则中优先级最高的动作，动作优先级从高到低的顺序为：丢弃 > 放行，但是对于生成日志动作只要匹配成功的规则中存在就会执行。
- 如果报文只与一个规则匹配成功，则执行此规则中指定的动作。
- 如果报文未与任何数据过滤规则匹配成功，则设备直接允许报文通过。

## 1.2 数据过滤配置任务简介

**表1-1 数据过滤配置任务简介**

| 配置任务 | 说明 | 详细配置 |
|---|---|---|
| 配置关键字组 | 必选 | 1.2.1 |
| 配置数据过滤策略 | 必选 | 1.2.2 |
| 在DPI应用profile中应用数据过滤策略 | 必选 | 1.2.3 |
| 激活DPI各业务模块的策略和规则配置 | 可选 | 1.2.4 |
| 基于安全策略应用数据过滤业务 | 二者至少选其一 | 1.2.5 |
| 基于对象策略应用数据过滤业务 | | 1.2.6 |

### 1.2.1 配置关键字组

一个关键字组中可配置多个数据过滤特征用于定义过滤报文应用层信息的字符串，各特征之间是或的关系。定义数据过滤特征的方式为正则表达式和文本两种。

**表1-2 配置关键字组**

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 创建关键字组，并进入关键字组视图 | **data-filter keyword-group** *keywordgroup-name* | 缺省情况下，不存在关键字组 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 配置关键字组的描述信息 | **description** *string* | 缺省情况下，不存在关键字组的描述信息 |
| 配置数据过滤特征 | **pattern** *pattern-name* { **regex** \| **text** } *pattern-string* | 缺省情况下，关键字组中不存在数据过滤特征 |

### 1.2.2 配置数据过滤策略

一个数据过滤策略中最多可以定义 32 个数据过滤规则，各规则之间是或的关系。每个规则中可配置一个关键字组、多种应用层协议类型、一种报文方向以及多个动作。

表1-3 配置数据过滤策略

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 创建数据过滤策略，并进入数据过滤策略视图 | **data-filter policy** *policy-name* | 缺省情况下，不存在数据过滤策略 |
| 配置数据过滤策略的描述信息 | **description** *string* | 缺省情况下，不存在数据过滤策略的描述信息 |
| 创建数据过滤规则，并进入数据过滤规则视图 | **rule** *rule-name* | 缺省情况下，不存在数据过滤规则 |
| 指定数据过滤规则采用的关键字组 | **keyword-group** *keywordgroup-name* | 缺省情况下，未指定数据过滤规则采用的关键字组 |
| 配置数据过滤规则的应用层协议类型 | **application** { **all** \| **type** { **ftp** \| **http** \| **smtp** } * } | 缺省情况下，数据过滤规则未指定应用层协议类型 |
| 配置数据过滤规则的匹配方向 | **direction** { **both** \| **download** \| **upload** } | 缺省情况下，数据过滤规则的匹配方向为会话的上传方向 |
| 配置数据过滤规则的动作 | **action** { **drop** \| **permit** } [ **logging** ] | 缺省情况下，数据过滤规则的动作为丢弃 |

### 1.2.3 在 DPI 应用 profile 中引用数据过滤策略

DPI 应用 porfile 是一个安全业务的配置模板，为实现数据过滤功能，必须在 DPI 应用 porfile 中引用指定的数据过滤策略。一个 DPI 应用 profile 中只能引用一个数据过滤策略，如果重复配置，则新的配置会覆盖已有配置。

表1-4 在 DPI 应用 profile 中引用数据过滤策略

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入DPI应用profile视图 | **app-profile** *profile-name* | 关于该命令的详细介绍请参见“DPI 深度安全命令参考”中的“应用层检测引擎” |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 在DPI应用profile中引用数据过滤策略 | **data-filter apply policy** *policy-name* | 缺省情况下，DPI应用profile中未引用数据过滤策略 |

### 1.2.4 激活 DPI 各业务模块的策略和规则配置

当DPI各业务模块的策略和规则被创建、修改和删除后，需要配置此功能使其策略和规则配置生效。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一配置此功能。

有关此功能的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

表1-5 激活 DPI 各业务模块的策略和规则配置

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 激活DPI各业务模块的策略和规则配置 | **inspect activate** | 缺省情况下，DPI各业务模块的策略和规则被创建、修改和删除时不生效 |

### 1.2.5 基于安全策略应用数据过滤业务

表1-6 基于安全策略应用数据过滤业务

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入安全策略视图 | **security-policy** { **ip** \| **ipv6** } | - |
| 进入安全策略规则视图 | **rule** { *rule-id* \| **name** *name* } * | - |
| 配置安全策略规则的动作为允许 | **action pass** | 缺省情况下，安全策略规则动作是丢弃 |
| 配置安全策略规则引用DPI应用profile | **profile** *app-profile-name* | 缺省情况下，安全策略规则中未引用DPI应用profile |

### 1.2.6 基于对象策略应用数据过滤业务

表1-7 基于对象策略应用数据过滤业务

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入对象策略视图 | **object-policy** { **ip** \| **ipv6** } *object-policy-name* | - |
| 在对象策略规则中引用DPI应用profile | **rule** [ *rule-id* ] **inspect** *app-profile-name* | 缺省情况下，在对象策略规则中未引用DPI应用profile |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 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** *source-zone-name* **destination** *destination-zone-name* | 缺省情况下，不存在安全域间实例<br>有关安全域间实例的详细介绍请参见“安全配置指导”中的“安全域” |
| 应用对象策略 | **object-policy apply** { **ip** \| **ipv6** } *object-policy-name* | 缺省情况下，安全域间实例内不应用对象策略 |

# 1.3 基于安全策略的数据过滤典型配置举例

## 1.3.1 数据过滤基本组网配置举例

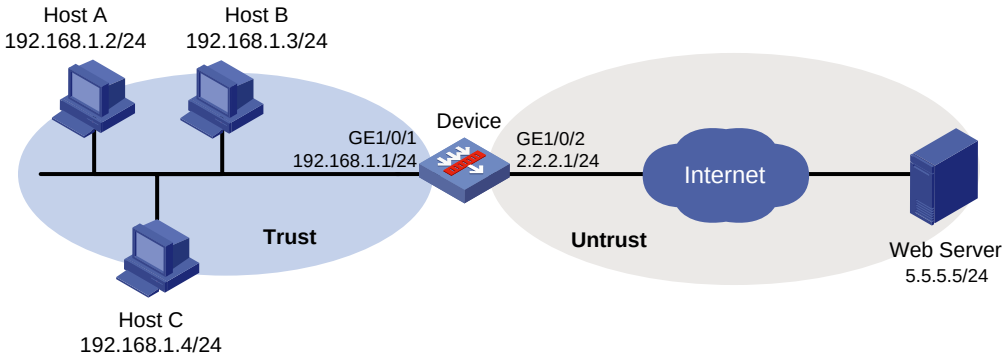
### 1. 组网需求

如图 1-1 所示，Device 分别通过 Trust 安全域和 Untrust 安全域与局域网和 Internet 相连。现有以下组网需求：

- 阻止 URI 或者 Body 字段含有“uri”或“abc.*abc”关键字的 HTTP 报文通过。
- 阻止下载文件内容中含有“www.abcd.com”关键字的 FTP 报文通过。
- 对以上被阻止的报文生成日志信息。

### 2. 组网图

图1-1 数据过滤基本组网配置组网图




### 3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域

# 向安全域 Trust 中添加接口 GigabitEthernet1/0/1。

```
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
```

# 向安全域 Untrust 中添加接口 GigabitEthernet1/0/2。

```
[Device] security-zone name untrust
```

```
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置对象组

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

```
[Device] object-group ip address datafilter
[Device-obj-grp-ip-datafilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-datafilter] quit
```

(4) 配置数据过滤功能

- 配置关键字组

# 创建关键字组 kg1，并进入关键字组视图。

```
[Device] data-filter keyword-group kg1
```

# 配置关键字文本 uri 和正则表示式 abc.*abc。

```
[Device-data-filter-kgroup-kg1] pattern 1 text uri
[Device-data-filter-kgroup-kg1] pattern 2 regex abc.*abc
[Device-data-filter-kgroup-kg1] quit
```

# 创建关键字组 kg2，并进入关键字组视图。

```
[Device] data-filter keyword-group kg2
```

# 配置匹配关键字文本 www.abcd.com。

```
[Device-data-filter-kgroup-kg2] pattern 1 text www.abcd.com
[Device-data-filter-kgroup-kg2] quit
```

- 配置数据过滤策略

# 创建数据过滤策略 p1，并进入数据过滤策略视图。

```
[Device] data-filter policy p1
```

# 创建数据过滤规则 r1，并进入数据过滤规则视图。

```
[Device-data-filter-policy-p1] rule r1
```

# 在规则 r1 中应用关键字组 kg1，配置应用类型为 HTTP，报文方向为会话的双向，动作为丢弃并输出日志。

```
[Device-data-filter-policy-p1-rule-r1] keyword-group kg1
[Device-data-filter-policy-p1-rule-r1] application type http
[Device-data-filter-policy-p1-rule-r1] direction both
[Device-data-filter-policy-p1-rule-r1] action drop logging
[Device-data-filter-policy-p1-rule-r1] quit
```

# 创建数据过滤规则 r2，并进入数据过滤策略视图。

```
[Device-data-filter-policy-p1] rule r2
```

# 在规则 r2 中应用关键字组 kg2，配置应用类型为 FTP，报文方向为会话的下载方向，动作为丢弃并输出日志。

```
[Device-data-filter-policy-p1-rule-r2] keyword-group kg2
[Device-data-filter-policy-p1-rule-r2] application type ftp
[Device-data-filter-policy-p1-rule-r2] direction download
[Device-data-filter-policy-p1-rule-r2] action drop logging
[Device-data-filter-policy-p1-rule-r2] quit
```

(5) 配置 DPI 应用 profile

# 创建名称为 profile1 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile profile1
```

# 在 DPI 应用 profile1 中应用数据过滤策略 p1。

```
[Device-app-profile-profile1] data-filter apply policy p1
[Device-app-profile-profile1] quit
```

# 激活 DPI 各业务模块的策略和规则配置。

```
[Device] inspect activate
```

(6) 配置安全策略引用数据过滤业务

# 进入 IPv4 安全策略视图

```
[Device] security-policy ip
```

# 创建名为 inspect1 的安全策略规则，过滤条件为：源安全域 Trust、源 IP 地址对象组 datafilter、目的安全域 Untrust。动作为允许，且引用的 DPI 应用 profile 为 profile1。

```
[Device-security-policy-ip] rule name inspect1
[Device-security-policy-ip-14-inspect1] source-zone trust
[Device-security-policy-ip-14-inspect1] source-ip datafilter
[Device-security-policy-ip-14-inspect1] destination-zone untrust
[Device-security-policy-ip-14-inspect1] action pass
[Device-security-policy-ip-14-inspect1] profile profile1
[Device-security-policy-ip-14-inspect1] quit
```

# 激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

#### 4. 验证配置

完成上述配置后，符合上述条件的 HTTP 报文和 FTP 报文将被阻断，并输出日志信息。

## 1.4 基于对象策略的数据过滤典型配置举例

### 1.4.1 数据过滤基本组网配置举例

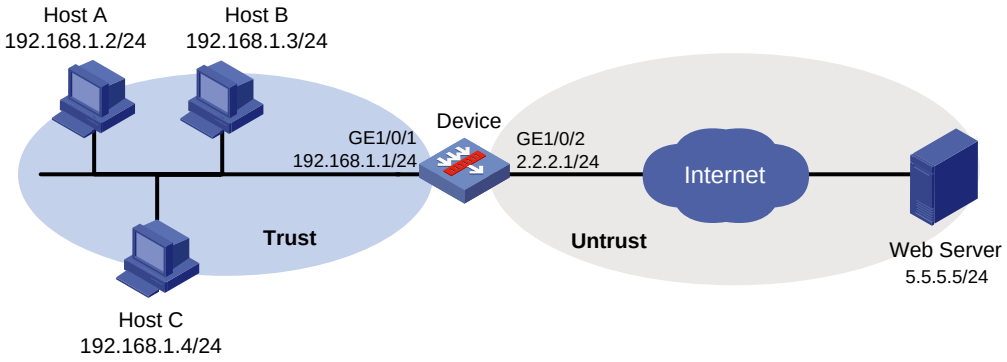
#### 1. 组网需求

如图 1-2 所示，Device 分别通过 Trust 安全域和 Untrust 安全域与局域网和 Internet 相连。现有以下组网需求：

- 阻止 URI 或者 Body 字段含有“uri”或“abc.*abc”关键字的 HTTP 报文通过。
- 阻止下载文件内容中含有“www.abcd.com”关键字的 FTP 报文通过。
- 对以上被阻止的报文生成日志信息。

## 2. 组网图

图1-2 数据过滤基本组网配置组网图




## 3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域

# 向安全域 Trust 中添加接口 GigabitEthernet1/0/1。

```
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
```

# 向安全域 Untrust 中添加接口 GigabitEthernet1/0/2。

```
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置对象组

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

```
[Device] object-group ip address datafilter
[Device-obj-grp-ip-datafilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-datafilter] quit
```

(4) 配置数据过滤功能

- 配置关键字组

# 创建关键字组 kg1，并进入关键字组视图。

```
[Device] data-filter keyword-group kg1
```

# 配置关键字文本 uri 和正则表示式 abc.*abc。

```
[Device-data-filter-kgroup-kg1] pattern 1 text uri
[Device-data-filter-kgroup-kg1] pattern 2 regex abc.*abc
[Device-data-filter-kgroup-kg1] quit
```

# 创建关键字组 kg2，并进入关键字组视图。

```
[Device] data-filter keyword-group kg2
```

# 配置匹配关键字文本 www.abcd.com。

```
[Device-data-filter-kgroup-kg2] pattern 1 text www.abcd.com
[Device-data-filter-kgroup-kg2] quit
```

- 配置数据过滤策略

# 创建数据过滤策略 p1，并进入数据过滤策略视图。

```
[Device] data-filter policy p1
```

# 创建数据过滤规则 r1，并进入数据过滤规则视图。

```
[Device-data-filter-policy-p1] rule r1
```

# 在规则 r1 中应用关键字组 kg1，配置应用类型为 HTTP，报文方向为会话的双向，动作为丢弃并输出日志。

```
[Device-data-filter-policy-p1-rule-r1] keyword-group kg1
[Device-data-filter-policy-p1-rule-r1] application type http
[Device-data-filter-policy-p1-rule-r1] direction both
[Device-data-filter-policy-p1-rule-r1] action drop logging
[Device-data-filter-policy-p1-rule-r1] quit
```

# 创建数据过滤规则 r2，并进入数据过滤策略视图。

```
[Device-data-filter-policy-p1] rule r2
```

# 在规则 r2 中应用关键字组 kg2，配置应用类型为 FTP，报文方向为会话的下载方向，动作为丢弃并输出日志。

```
[Device-data-filter-policy-p1-rule-r2] keyword-group kg2
[Device-data-filter-policy-p1-rule-r2] application type ftp
[Device-data-filter-policy-p1-rule-r2] direction download
[Device-data-filter-policy-p1-rule-r2] action drop logging
[Device-data-filter-policy-p1-rule-r2] quit
```

(5) 配置 DPI 应用 profile

# 创建名称为 profile1 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile profile1
```

# 在 DPI 应用 profile1 中应用数据过滤策略 p1。

```
[Device-app-profile-profile1] data-filter apply policy p1
[Device-app-profile-profile1] quit
```

# 激活 DPI 各业务模块的策略和规则配置。

```
[Device] inspect activate
```

(6) 配置对象策略

# 创建名为 inspect1 的对象策略，并进入对象策略视图。

```
[Device] object-policy ip inspect1
```

# 对源 IP 地址对象组 datafilter 对应的报文进行深度检测，引用的 DPI 应用 profile 为 profile1。

```
[Device-object-policy-ip-inspect1] rule inspect profile1 source-ip datafilter
destination-ip any
[Device-object-policy-ip-inspect1] quit
```

(7) 配置安全域间实例并应用对象策略

# 创建源安全域 Trust 到目的安全域 Untrust 的安全域间实例，并应用对源 IP 地址对象组 datafilter 对应的报文进行深度检测的对象策略 inspect1。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-trust-untrust] object-policy apply ip inspect1
[Device-zone-pair-security-trust-untrust] quit
```

### 4. 验证配置

完成上述配置后，符合上述条件的 HTTP 报文和 FTP 报文将被阻断，并输出日志信息。