目 录

1 ASPF配置

1.1 ASPF简介

包过滤防火墙属于静态防火墙，目前存在的问题如下：

- 对于传输层协议，配置管理员无法精确预知反向回应报文信息，因此增加了包过滤配置的难度。同时，若配置管理员配置了比较宽松的放行策略，则会增加内网被攻击的风险。
- 对于多通道的应用层协议（如 FTP 等），部分安全策略配置无法预知。
- 无法跟踪传输层和应用层的协议状态，无法检测某些来自传输层和应用层的攻击行为。
- 无法识别来自网络中伪造的 ICMP 差错报文，从而无法避免 ICMP 的恶意攻击。

因此，提出了状态防火墙——ASPF（Advanced Stateful Packet Filter，高级状态包过滤）的概念。ASPF 能够实现的主要功能有：

- 应用层协议检测：检查应用层协议信息，如报文的协议类型和端口号等信息，并且监控每一个连接的应用层协议状态。对于所有连接，每一个连接状态信息都将被 ASPF 维护，并用于动态地决定数据包是否被允许通过防火墙进入内部网络，以阻止恶意的入侵。
- 传输层协议检测：检测传输层协议信息，包括 TCP 协议、UDP 协议、UDP-Lite 协议、SCTP 协议、Raw IP 协议、ICMP 协议、ICMPv6 协议和 DCCP 协议。例如 TCP/UDP 检测，能够根据源、目的地址及端口号决定 TCP 或 UDP 报文是否可以通过防火墙进入内部网络。
- ICMP 差错报文检测：正常 ICMP 差错报文中均携带有本报文对应连接的相关信息，根据这些信息可以匹配到相应的连接。如果匹配失败，则根据当前配置决定是否丢弃该 ICMP 报文。
- TCP 连接首包检测：对 TCP 连接的首报文进行检测，查看是否为 SYN 报文，如果不是 SYN 报文则根据当前配置决定是否丢弃该报文。缺省情况下，不丢弃非 SYN 首包，适用于不需要严格 TCP 协议状态检查的组网场景。例如当防火墙设备首次加入网络时，网络中原有 TCP 连接的非首包在经过新加入的设备时如果被丢弃，会中断已有的连接，造成不好的用户体验，因此建议暂且不丢弃非 SYN 首包，等待网络拓扑稳定后，再开启非 SYN 首包丢弃功能。

在网络边界，ASPF 和包过滤防火墙协同工作，包过滤防火墙负责按照 ACL 规则进行报文过滤（阻断或放行），ASPF 负责对已放行报文进行信息记录，使已放行的报文的回应报文可以正常通过配置了包过滤防火墙的接口。因此，ASPF 能够为企业内部网络提供更全面的、更符合实际需求的安全策略。

1.1.1 ASPF基本概念

1. 单通道协议和多通道协议

ASPF 将应用层协议划分为：

- 单通道协议：完成一次应用的全过程中，只有一个连接参与数据交互，如 SMTP、HTTP。
- 多通道协议：完成一次应用的全过程中，需要多个连接配合，即控制信息的交互和数据的传送需要通过不同的连接完成的，如 FTP。

2. 内部接口和外部接口

如果设备连接了内部网络和外部网络，并且要通过部署 ASPF 来保护内部网络中的主机和服务器，则设备上与内部网络连接的接口就称为内部接口，与外部网络相连的接口就称为外部接口。

若需要保护内部网络，则可以将 ASPF 应用于设备外部接口的出方向或者应用于设备内部接口的入方向。

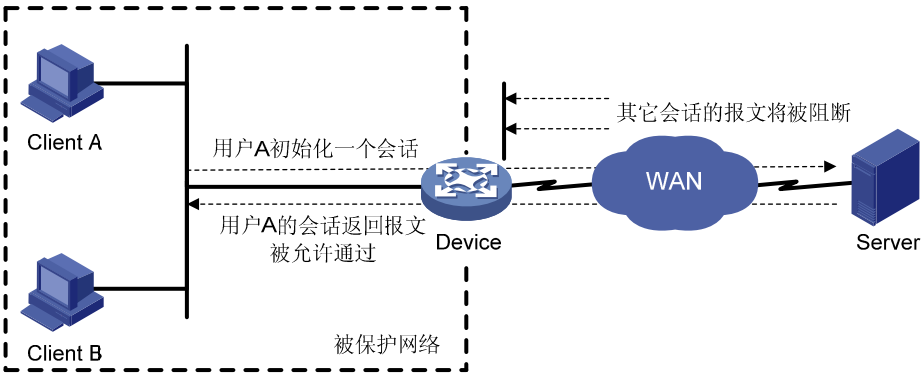
3. 安全域间实例

安全域间实例用于指定 ASPF 需要检测的业务流的源安全域和目的安全域，它们分别描述了经过网络设备的业务流的首个数据包要进入的安全域和要离开的安全域。关于安全域的详细介绍，请参见“基础配置指导”中的“安全域”。

1.1.2 ASPF检测原理

1. 应用层协议检测基本原理

图1-1 应用层协议检测基本原理示意图



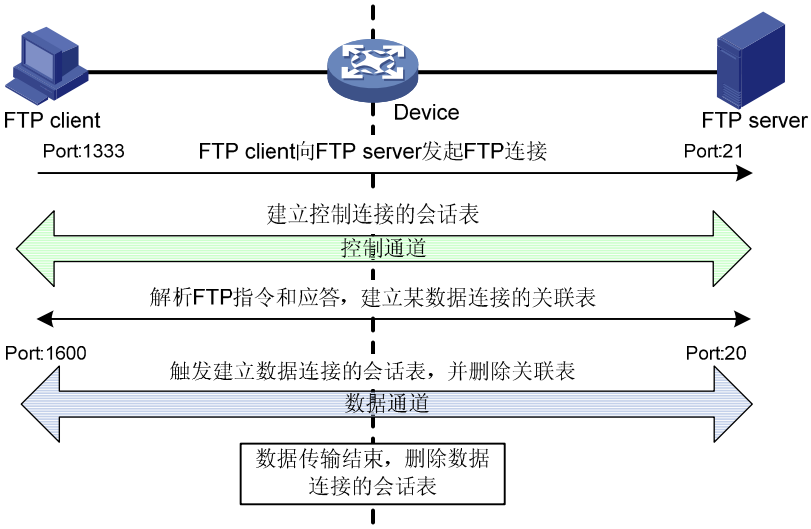
如 图 1-1 所示，为了保护内部网络，可以在边界设备上配置访问控制列表，以允许内部网络的主机访问外部网络，同时拒绝外部网络的主机访问内部网络。但是访问控制列表会将用户发起连接后返回的报文过滤掉，导致连接无法正常建立。利用ASPF的应用层协议检测可以解决此问题。

当在设备上配置了应用层协议检测后，ASPF 可以检测每一个应用层的连接，具体检测原理如下：

- 对于单通道协议，ASPF 在检测到第一个向外发送的报文时创建一个会话表项。该会话表项中记录了对应的正向报文信息和反向报文信息，用于维护会话状态并检测会话状态的转换是否正确。匹配某条会话表项的所有报文都将免于接受静态包过滤策略的检查。
- 对于多通道协议，ASPF 除了创建会话表项之外，还会根据协议的协商情况，创建一个或多个关联表项，用于关联属于同一个应用业务的不同会话。关联表项在多通道协议协商的过程中创建，在多通道协议协商完成后删除。关联表项主要用于匹配会话首报文，使已通过协商的会话报文可免于接受静态包过滤策略的检查。

单通道应用层协议（如 HTTP）的检测过程比较简单，当发起连接时建立会话表项，连接删除时随之删除会话表项即可。下面以 FTP 检测为例说明多通道应用层协议检测的过程。

图1-2 FTP 检测过程示意图



如 图 1-2 所示，FTP连接的建立过程如下：假设FTP client以 1333 端口向FTP server的 21 端口发起FTP控制通道的连接，通过协商决定在FTP server的 20 端口与FTP Client的 1600 端口之间建立数据通道，并由FTP server发起数据连接，数据传输超时或结束后数据通道删除。

FTP 检测在 FTP 连接建立到拆除过程中的处理如下：

(1) 检查 FTP client 向 FTP server 发送的 IP 报文，确认为基于 TCP 的 FTP 报文。检查端口号，确认该连接为 FTP client 与 FTP server 之间的控制连接，建立会话表项。

(2) 检查 FTP 控制连接报文，根据会话表项进行 TCP 状态检测。解析 FTP 指令，如果包含数据通道建立指令，则创建关联表项描述对应数据连接的特征。

(3) 对于返回的 FTP 控制连接报文，根据会话表项进行 TCP 状态检测，检测结果决定是否允许报文通过。

(4) FTP 数据连接报文通过设备时，将会触发建立数据连接的会话表项，并删除所匹配的关联表项。

(5) 对于返回的 FTP 数据连接报文，则通过匹配数据连接的会话表项进行 TCP 状态检测，检查结果决定是否允许报文通过。

(6) 数据连接结束时，数据连接的会话表项将被删除。FTP 连接删除时，控制连接的会话表项也会被删除。

2. 传输层协议检测基本原理

传输层协议检测通过建立会话表项记录报文的传输层信息，如源地址、目的地址及端口号等，达到动态放行报文的目的。

传输层协议检测要求返回到 ASPF 外部接口的报文要与之前从 ASPF 外部接口发出去的报文完全匹配，即源地址、目的地址及端口号完全对应，否则返回的报文将被丢弃。因此对于 FTP 这样的多通道应用层协议，在不配置应用层检测而直接配置 TCP 检测的情况下会导致数据连接无法建立。

1.1.3 ASPF配置限制和指导

如果设备上其他业务模块开启 ALG 功能时，即便未配置多通道应用层协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。例如：开启 DPI 相关业务功能时会打开 ALG 功能，此时 DPI 处理的多通道协议（如 SIP 等）报文进行 ASPF 处理时，即便未配置 SIP 协议的 ASPF 检测，SIP 协议的数据连接也可以建立成功；开启 NAT ALG 功能时，即便未配置多通道协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。

1.2 ASPF配置任务简介

表1-1 ASPF 配置任务简介

配置任务	说明	详细配置
配置ASPF策略	必选	1.3
在接口上应用ASPF策略	必选	1.4
在安全域间实例上应用ASPF策略	必选	1.5
开启域间策略丢包时发送ICMP差错报文功能	可选	1.6

1.3 配置ASPF策略

若配置了 **detect** 命令，则对报文的应用层协议进行 ASPF 检查；若没有配置 **detect** 命令，则仅对报文的传输层协议进行 ASPF 检查。

如果设备上其他业务模块开启 ALG 功能时，即便未配置多通道应用层协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。例如：开启 DPI 相关业务功能时会打开 ALG 功能，此时 DPI 处理的多通道协议（如 SIP 等）报文进行 ASPF 处理时，即便未配置 SIP 协议的 ASPF 检测，SIP 协议的数据连接也可以建立成功；开启 NAT ALG 功能时，即便未配置多通道协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。但是在设备上未配置 DPI（Deep Packet Inspection，深度报文检测）相关业务功能只配置了 ASPF 功能的情况下，必须配置 **detect** 命令，否则会导致数据连接无法建立。**detect** 命令支持的应用层协议中除 HTTP、SMTP 和 TFTP 之外的所有应用层协议均为多通道应用层协议。

ASPF 策略默认已经开启对传输层协议的检测，无需进行配置，也不能修改。

可以根据需要在 ASPF 策略中配置应用层协议检测。目前，设备对于部分应用层协议（FTP、H323、HTTP、SCCP、SIP、SMTP），还支持进行协议状态合法性检查功能，对不符合协议状态的报文进行丢弃。对于其它应用层协议，仅进行连接状态信息的维护，不做协议状态合法性检查。

表1-2 配置 ASPF 策略

操作	命令	说明
进入系统视图	**system-view**	-
创建ASPF策略，并进入ASPF策略视图	**aspf policy** *aspf-policy-number*	缺省情况下，不存在ASPF策略

操作	命令	说明
（可选）为应用层协议配置ASPF检测	**detect** { **ftp** | **h323** | **sccp** | **sip** } | **gtp** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sqlnet** | **tftp** | **xdmcp** }	缺省情况下，未配置应用层协议的ASPF检测
（可选）开启ICMP差错报文丢弃功能	**icmp-error drop**	缺省情况下，不丢弃ICMP差错报文
（可选）开启非SYN的TCP首报文丢弃功能	**tcp syn-check**	缺省情况下，不丢弃非SYN的TCP首报文

1.4 在接口上应用ASPF策略

只有将定义好的 ASPF 策略应用到接口的出或入方向上，才能对通过接口的特定方向的流量进行检测。在处理入接口报文时需要查找对应接口入方向的策略；在处理出接口报文时需要查找对应接口出方向的策略。如果接口应用了 ASPF 策略，所有进入或离开该接口的报文都需要与会话表项进行匹配，查找不到与之匹配的会话表项时会触发创建会话表。

如果 ASPF 与包过滤防火墙协同工作，可以在外部接口或内部接口的入方向或出方向上配置特定的 ASPF 和包过滤策略，根据特定配置，可以拒绝外部网络上的用户对内部网络的主动访问，但内部网络的用户访问外部网络时，返回的报文可以按照外部接口出方向或内部接口入方向上的 ASPF 配置进行 ASPF 检测。

由于 ASPF 对于应用层协议状态的保存和维护都是基于接口的，因此在实际应用中，必须保证报文入口的一致性，即必须保证连接发起方发送的报文和响应端返回的报文经过同一接口。

表1-3 在接口上应用 ASPF 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上应用ASPF策略	**aspf apply policy** *aspf-policy-number* { **inbound** | **outbound** }	缺省情况下，接口上没有应用ASPF策略

1.5 在安全域间实例上应用ASPF策略

只有将定义好的 ASPF 策略应用到安全域间实例上，才能对通过安全域间实例的流量进行检测。如果安全域间实例上应用了 ASPF 策略，所有通过该域间实例的报文都需要与会话表项进行匹配，查找不到与之匹配的会话表项并且符合包过滤放行条件时会触发创建会话表。

在域间实例上 ASPF 必须与包过滤防火墙协同工作：通过在域间实例上应用包过滤策略，可以允许源安全域的用户主动访问目的安全域所连接网络；通过在域间实例上应用 ASPF 策略，由 ASPF 策略对源安全域用户访问目的安全域的报文以及对应的反向报文进行检测和放行。

表1-4 在安全域间实例上应用 ASPF 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入安全域间实例视图	**zone-pair security source** *source-zone-name* **destination** *destination-zone-name*	关于安全域间实例的具体配置，请参见“基础命令参考”中的“安全域”。
在安全域间实例上应用ASPF策略	**aspf apply policy** *aspf-policy-number*	缺省情况下，安全域间实例上应用了一个缺省的ASPF策略，该策略支持对所有传输层协议和FTP协议报文进行ASPF检测，但是ICMP差错报文检查功能和非SYN的TCP首报文丢弃功能处于关闭状态

1.6 开启域间策略丢包时发送ICMP差错报文功能

缺省情况下，设备在安全域间实例下配置安全域间策略，丢弃不符合策略的报文，但不发送 ICMP 差错报文，这样可以减少网络上的无用报文，节约带宽。

使用 traceroute 功能时用到 ICMP 差错报文，需要开启发送 ICMP 差错报文的功能。

表1-5 开启域间策略丢包时发送 ICMP 差错报文功能

操作	命令	说明
进入系统视图	**system-view**	-
开启域间策略丢包时发送ICMP差错报文功能	**aspf icmp-error reply**	缺省情况下，在域间策略丢包时，设备不发送ICMP差错报文

1.7 ASPF显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ASPF 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 ASPF 的统计信息。

表1-6 ASPF 显示和维护

操作	命令
查看ASPF策略配置信息及应用ASPF策略的信息	**display aspf all**
查看接口上的ASPF策略信息	**display aspf interface**
查看ASPF策略的配置信息	**display aspf policy** { *aspf-policy-number* | **default** }
查看ASPF的会话表信息（独立运行模式）	**display aspf session** [**ipv4** | **ipv6**] [**slot** *slot-number*] [**verbose**]
查看ASPF的会话表信息（IRF模式）	**display aspf session** [**ipv4** | **ipv6**] [**chassis** *chassis-number* **slot** *slot-number*] [**verbose**]

操作	命令
删除ASPF的会话表（独立运行模式）	**reset aspf session** [**ipv4 | ipv6**] [**slot** *slot-number*]
删除ASPF的会话表（IRF模式）	**reset aspf session** [**ipv4 | ipv6**] [**chassis** *chassis-number* **slot** *slot-number*]

1.8 ASPF典型配置举例

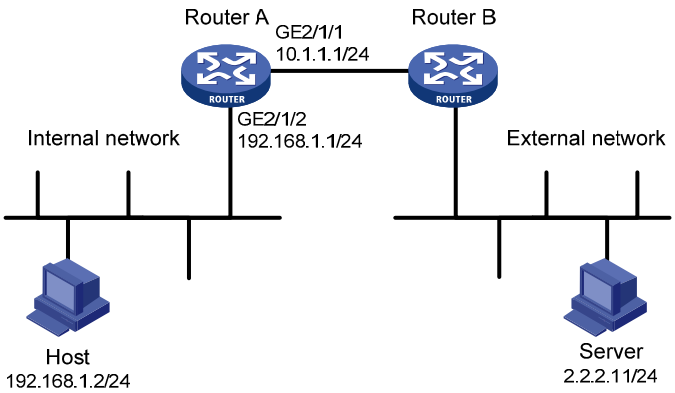
1.8.1 检测FTP应用的ASPF典型配置举例

1. 组网需求

Router A 为连接内部网络与外部网络的边界设备，内部网络中的本地用户需要访问外部网络提供的 FTP 服务。要求配置 ASPF 策略，检测通过 Router A 的 FTP 流量。如果该报文是内部网络用户发起的 FTP 连接的返回报文，则允许其通过 Router A 进入内部网络，其它报文被禁止。

2. 组网图

图1-3 检测 FTP 应用的 ASPF 典型配置组网图



3. 配置步骤

配置 ACL 3111，定义规则：拒绝所有 IP 流量进入内部网络。

```
<RouterA> system-view
[RouterA] acl advanced 3111
[RouterA-acl-ipv4-adv-3111] rule deny ip
[RouterA-acl-ipv4-adv-3111] quit
```

创建 ASPF 策略 1，配置检测应用层协议 FTP。

```
[RouterA] aspf policy 1
[RouterA-aspf-policy-1] detect ftp
[RouterA-aspf-policy-1] quit
```

在接口 GigabitEthernet2/1/1 的入方向上应用包过滤策略，拒绝所有 IP 流量进入内部网络。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 3111 inbound
```

在接口 GigabitEthernet2/1/1 的出方向上应用 ASPF 策略，ASPF 会为内部网络和外部网络之间的 FTP 连接创建会话表项，并允许匹配该表项的外部网络返回报文进入内部网络。

```
[RouterA-GigabitEthernet2/1/1] aspf apply policy 1 outbound
```

4. 验证配置

以上配置完成后，从 Host 向 Server 发起的 FTP 连接可正常建立，而从外部网络发起连接的报文则无法进入内部网络。在 Router A 上可以查看到已经建立的 ASPF 会话。

```
<RouterA> display aspf session ipv4
Initiator:
  Source      IP/port: 192.168.1.2/1877
  Destination IP/port: 2.2.2.11/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/1/1

Total sessions found: 1
```

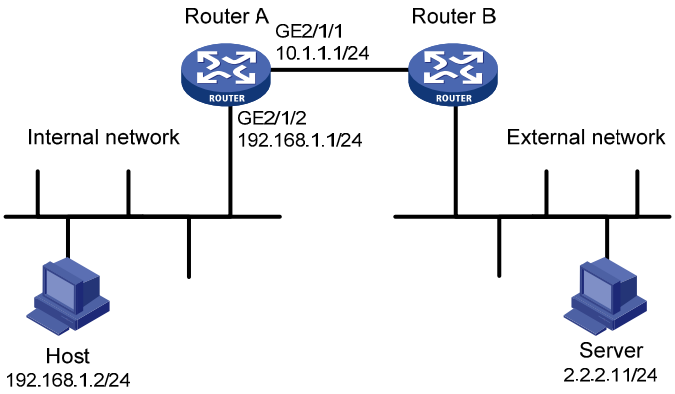
1.8.2 检测ICMP和SYN报文的ASPF典型配置举例

1. 组网需求

Router A 为连接内部网络与外部网络的边界设备，内部网络中的本地用户需要访问外部网络。为避免来自外部网络的 ICMP 和 SYN 报文的恶意攻击，要求在 Router A 上配置 ASPF 策略，实现 ICMP 差错报文检测及 TCP 非 SYN 首报文丢弃功能。

2. 组网图

图1-4 检测 ICMP 和 SYN 报文的 ASPF 典型配置组网图



3. 配置步骤

配置 ACL 3111，定义规则：拒绝所有 IP 流量进入内部网络。

```
<RouterA> system-view
[RouterA] acl advanced 3111
[RouterA-acl-ipv4-adv-3111] rule deny ip
[RouterA-acl-ipv4-adv-3111] quit
```

创建 ASPF 策略 1。

```
[RouterA] aspf policy 1
```

设置 ASPF 策略 1 丢弃 ICMP 差错报文。

```
[RouterA-aspf-policy-1] icmp-error drop
```

设置 ASPF 策略 1 丢弃非 SYN 的 TCP 首报文。

```
[RouterA-aspf-policy-1] tcp syn-check
```

配置 ASPF 策略 1 检测应用层协议 FTP。（此处仅为示例，可根据实际组网配置需要检测的协议）

```
[RouterA-aspf-policy-1] detect ftp
[RouterA-aspf-policy-1] quit
```

在接口 GigabitEthernet2/1/1 的入方向上应用包过滤策略，拒绝所有 IP 流量进入内部网络。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 3111 inbound
```

在接口 GigabitEthernet2/1/1 的出方向上应用 ASPF 策略。

```
[RouterA-GigabitEthernet2/1/1] aspf apply policy 1 outbound
```

4. 验证配置

查看策略号为 1 的 ASPF 策略的配置信息。

```
<RouterA> display aspf policy 1
ASPF policy configuration:
  Policy number: 1
    ICMP error message check: Enabled
    TCP SYN packet check: Enabled
    Inspected protocol
      FTP
```

通过以上配置，Router A 能够识别出来自网络中伪造的 ICMP 差错报文，可以避免 ICMP 的恶意攻击，而且非 SYN 报文的 TCP 首包也将被丢弃。

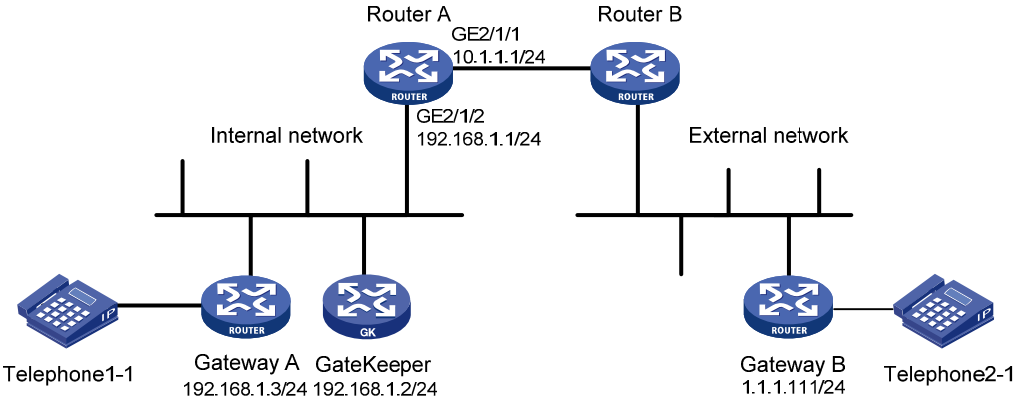
1.8.3 ASPF支持H.323 应用典型配置举例

1. 组网需求

在如 图 1-5 所示的一种常见的H.323 典型组网应用中，Router A为连接内部网络与外部网络的边界设备，外部网络中的Gateway B需要访问内部网络中的H.323 GateKeeper，并通过GateKeeper的协助，与内网中的H.323 端点Gateway A建立呼叫连接。要求配置ASPF策略，检测通过Router A的H.323 协议报文，允许外部网络设备主动访问内部网络的GateKeeper，并通过与其协商进而实现访问Gateway A，其它协议的外部网络报文均被禁止。

2. 组网图

图1-5 ASPF 支持 H.323 典型配置组网图



3. 配置步骤

配置 ACL 3200，定义规则：拒绝所有除访问 GateKeeper 之外的 IP 流量进入内部网络。

```
<RouterA> system-view
[RouterA] acl advanced 3200
[RouterA-acl-ipv4-adv-3200] rule 0 permit ip destination 192.168.1.2 0
[RouterA-acl-ipv4-adv-3200] rule 5 deny ip
[RouterA-acl-ipv4-adv-3200] quit
```

创建 ASPF 策略 1，配置检测应用层协议 H.323。

```
[RouterA] aspf policy 1
[RouterA-aspf-policy-1] detect h323
[RouterA-aspf-policy-1] quit
```

在接口 GigabitEthernet2/1/1 的入方向上应用包过滤策略，拒绝所有除访问 GateKeeper 之外的流量进入内部网络。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 3200 inbound
```

在接口 GigabitEthernet2/1/1 的入方向上应用 ASPF 策略，ASPF 会为内部网络和外部网络之间的 H.323 连接创建会话表项，并允许匹配该表项的外部网络返回报文进入内部网络。

```
[RouterA-GigabitEthernet2/1/1] aspf apply policy 1 inbound
[RouterA-GigabitEthernet2/1/1] quit
```

4. 验证配置

以上配置完成后，从 Gateway B 向 GateKeeper 发起的 H.323 连接以及从 Gateway B 向 Gateway A 发起的 H323 连接均可正常建立，但外部网络发起的其它协议的报文则无法进入内部网络。在 Router A 上可以查看到已经建立的 ASPF 会话。

```
[RouterA] display aspf session ipv4
Initiator:
  Source      IP/port: 1.1.1.111/33184
  Destination IP/port: 192.168.1.3/32828
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet2/1/1

Initiator:
  Source      IP/port: 1.1.1.111/1719
  Destination IP/port: 192.168.1.2/1719
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet2/1/1

Initiator:
  Source      IP/port: 1.1.1.111/3521
  Destination IP/port: 192.168.1.2/20155
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/1/1

Initiator:
```

```
  Source      IP/port: 1.1.1.111/33185
  Destination IP/port: 192.168.1.3/32829
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet2/1/1

Initiator:
  Source      IP/port: 1.1.1.111/3688
  Destination IP/port: 192.168.1.2/1720
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/1/1

Total sessions found: 5
```

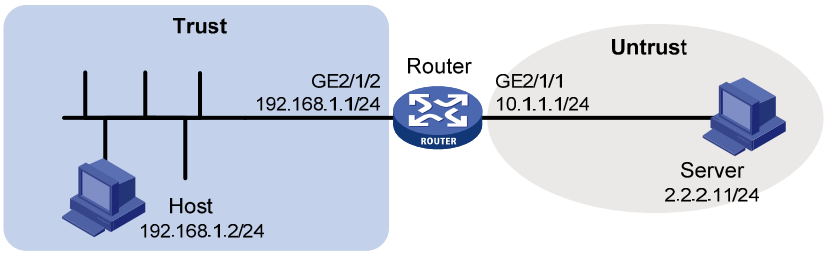
1.8.4 安全域间实例上的ASPF典型配置举例

1. 组网需求

Router 为连接内部网络与外部网络的边界设备，内部网络中的本地用户需要访问外部网络提供的应用（例如 FTP）服务。要求配置 ASPF 策略，检测通过 Router 的流量。如果该报文是内部网络用户发起的应用（例如 FTP）连接的返回报文，则允许其通过 Router 进入内部网络，其它外部主动访问内部网络的报文被禁止。

2. 组网图

图1-6 检测应用的 ASPF 典型配置组网图



3. 配置步骤

配置 ACL 3500，定义规则：允许内部 IP 流量访问外部网络（如果只允许某种应用的报文通过，可以配置更细化的 rule）。

```
<Router> system-view
[Router] acl advanced 3500
[Router-acl-ipv4-adv-3500] rule permit ip
[Router-acl-ipv4-adv-3500] quit
```

向安全域 Trust 中添加三层接口 GigabitEthernet2/1/2。

```
[Router] security-zone name trust
[Router-security-zone-Trust] import interface gigabitethernet 2/1/2
[Router-security-zone-Trust] quit
```

向安全域 Untrust 中添加三层接口 GigabitEthernet2/1/1。

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

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

创建 ASPF 策略 1，配置检测应用层协议 FTP。

```
[Router] aspf policy 1
[Router-aspf-policy-1] detect ftp
[Router-aspf-policy-1] quit
```

在安全域间实例上应用包过滤策略，放行内部 IP 流量访问外部网络。

```
[Router] zone-pair security source trust destination untrust
[Router-zone-pair-security-Trust-Untrust] packet-filter 3500
```

在安全域间实例上应用 ASPF 策略，ASPF 会为内部网络和外部网络之间的符合包过滤策略的连接创建会话表项，并允许匹配该表项的外部网络返回报文进入内部网络。

```
[Router-zone-pair-security-Trust-Untrust] aspf apply policy 1
[Router-zone-pair-security-Trust-Untrust] quit
```

4. 验证配置

以上配置完成后，从 Host 向 Server 发起的 FTP 连接可正常建立，而从外部网络发起连接的报文则无法进入内部网络。在 Router 上可以查看到已经建立的 ASPF 会话。

```
<Router> display aspf session ipv4
Initiator:
  Source      IP/port: 192.168.1.2/1877
  Destination IP/port: 2.2.2.11/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/1/2
  Source security zone: Trust

Total sessions found: 1
```