H3C 防火墙会话管理特性技术介绍

ISSUE 1.0

课程目标

学习完本课程，您应该能够：

- 熟悉会话管理技术概述及实现原理
- 熟悉会话管理典型配置和应用场景
- 熟悉会话管理常见问题和注意事项

目录

会话管理技术需求背景

- **重要的基础性软件模块**
  - → 会话管理是为了实现NAT、ASPF、连接数限制、攻击检测、负载均衡、应用层检测等等基于会话进行处理的业务而抽象出来的公共功能。能够处理各种会话信息，根据会话状态对信息执行老化处理，并提供给其它业务模块一个统一的信息查询接口。把传输层报文之间的交互关系抽象为会话，并根据发起方或响应方的报文信息对会话进行状态更新和超时老化
- **会话管理的本质**
  - → 会话管理主要基于传输层协议对报文进行检测。其实质是通过检测传输层协议信息（即通用TCP协议和UDP协议）来对连接的状态进行跟踪，并对所有连接的状态信息进行统一维护和管理

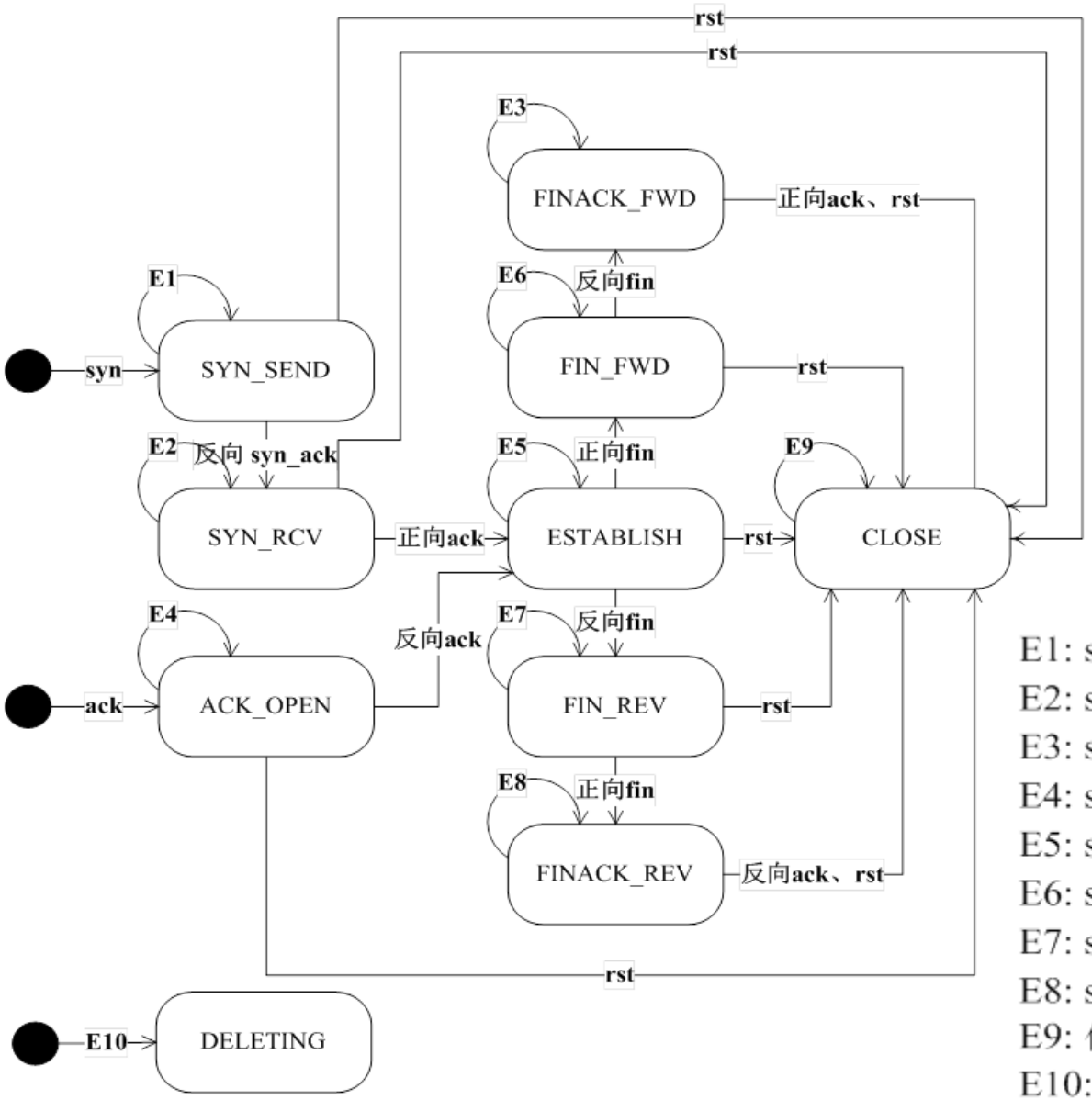
会话管理概念

- **所谓流（Flow），**是一个单方向的概念，根据报文所携带的三元组或者五元组唯一标识。根据IP层协议的不同，流分为四类：
  - → TCP流：通过五元组唯一标识
  - → UDP流：通过五元组唯一标识
  - → ICMP流：通过三元组 + ICMP type + ICMP code唯一标识
  - → RAW IP流：非TCP/UDP/ICMP的其它IP协议，通过三元组标识
- **所谓会话（Session），**是一个双向的概念，一个会话关联两个方向的流，一个为会话发起方（Initiator），另一个为会话响应方（Responder）。通过会话所属的任一方向的流特征都可以唯一确定该会话及方向

会话管理特性的主要功能

- 会话表项的管理
- 会话四层协议状态管理
- 应用层报文协议识别
- 支持不同的协议状态和应用层会话动态超时老化时间
- 支持指定特征会话维持长连接
- 会话四层协议CHECKSUM检查
- 为需要端口协商的应用层协议提供报文匹配(关联表)
- 支持ICMP差错控制报文解析以及到会话的匹配

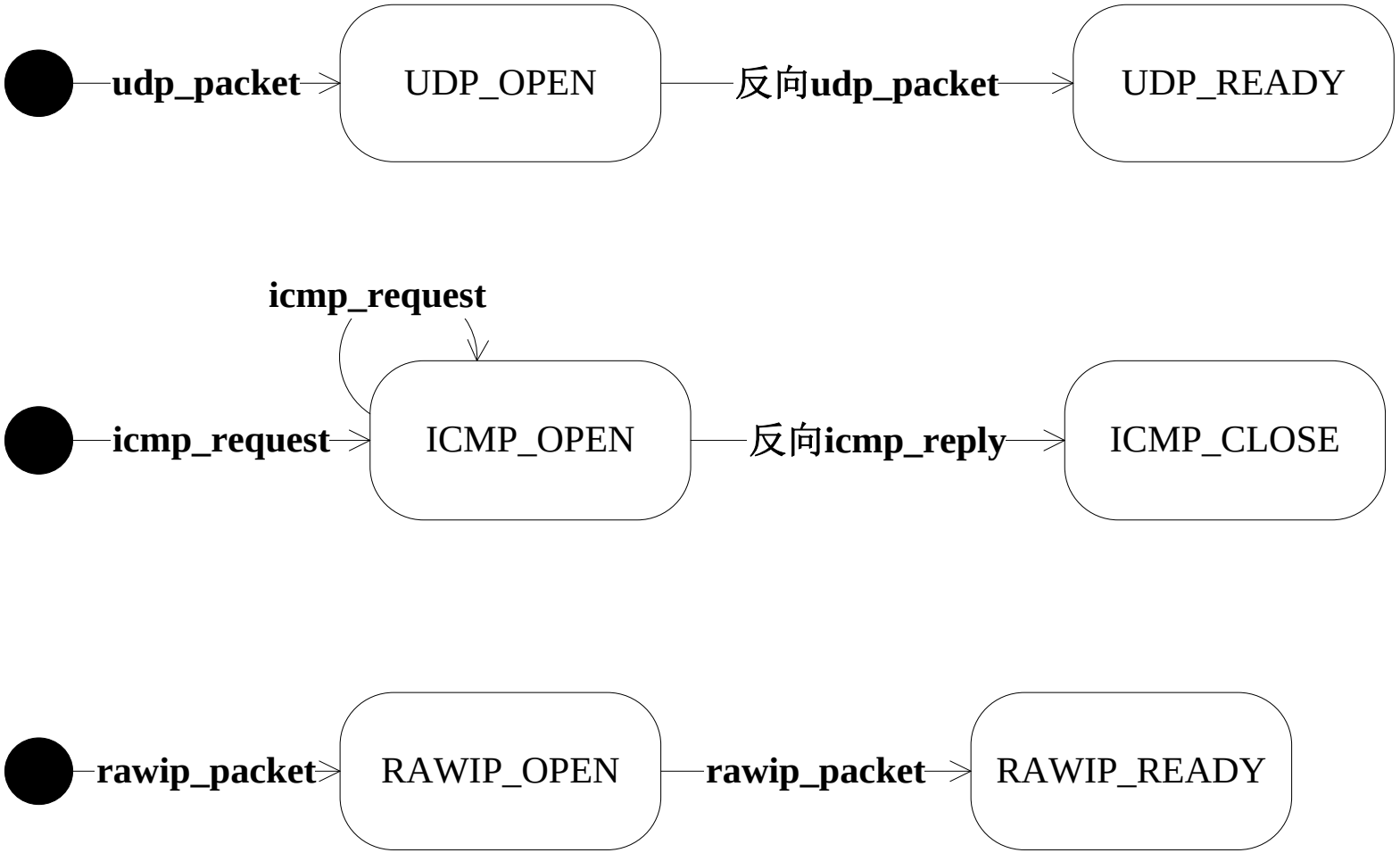
TCP会话状态机



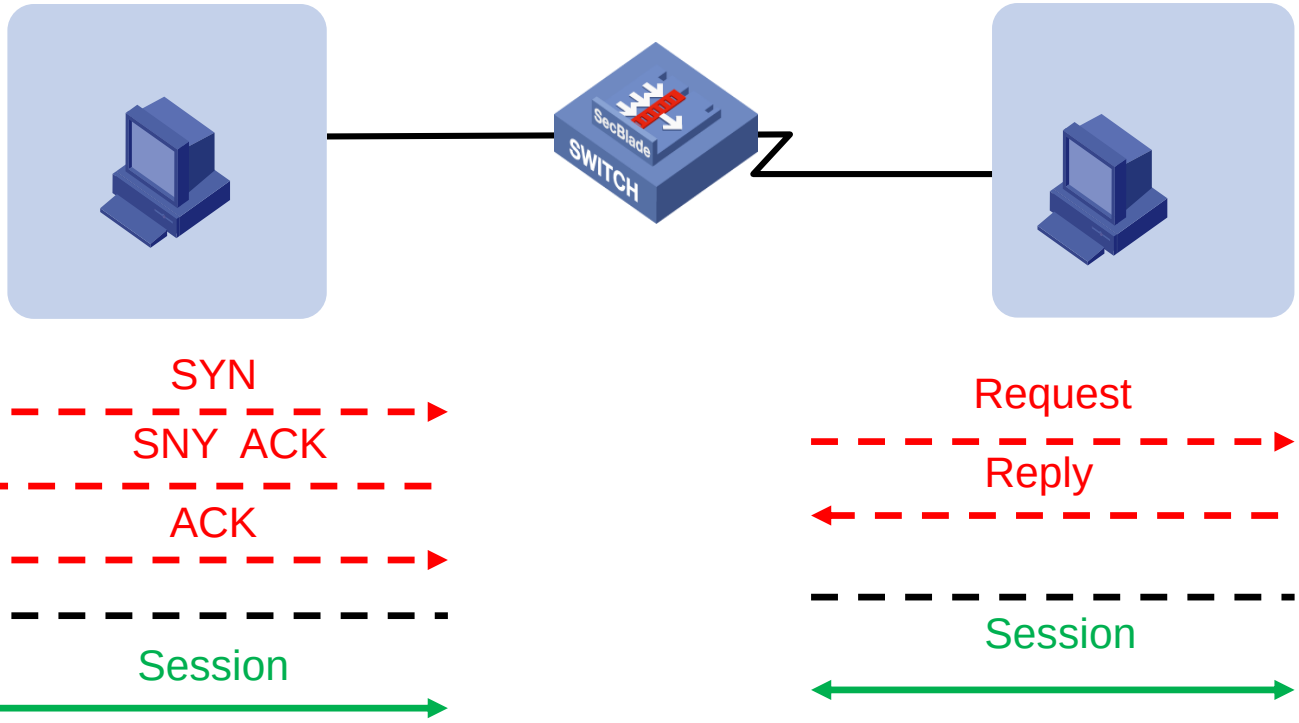
- 创建及删除会话
- 对会话的状态进行跟踪，提供判断报文是否符合协议状态的依据

E1: syn、ack、正向syn_ack、fin、none
E2: syn、反向ack、syn ack、fin、none
E3: syn、反向ack、syn_ack、fin、none
E4: syn、正向ack、syn_ack、fin、none
E5: syn、ack、syn_ack、none
E6: syn、ack、syn_ack、正向fin、none
E7: syn、ack、syn_ack、反向fin、none
E8: syn、正向ack、syn_ack、fin、none
E9: 任何报文类型
E10: syn_ack、fin、rst、none

UDP/ICMP/RAW_IP会话状态机



会话的创建



TCP Session

UDP/ICMP/Raw IP Session

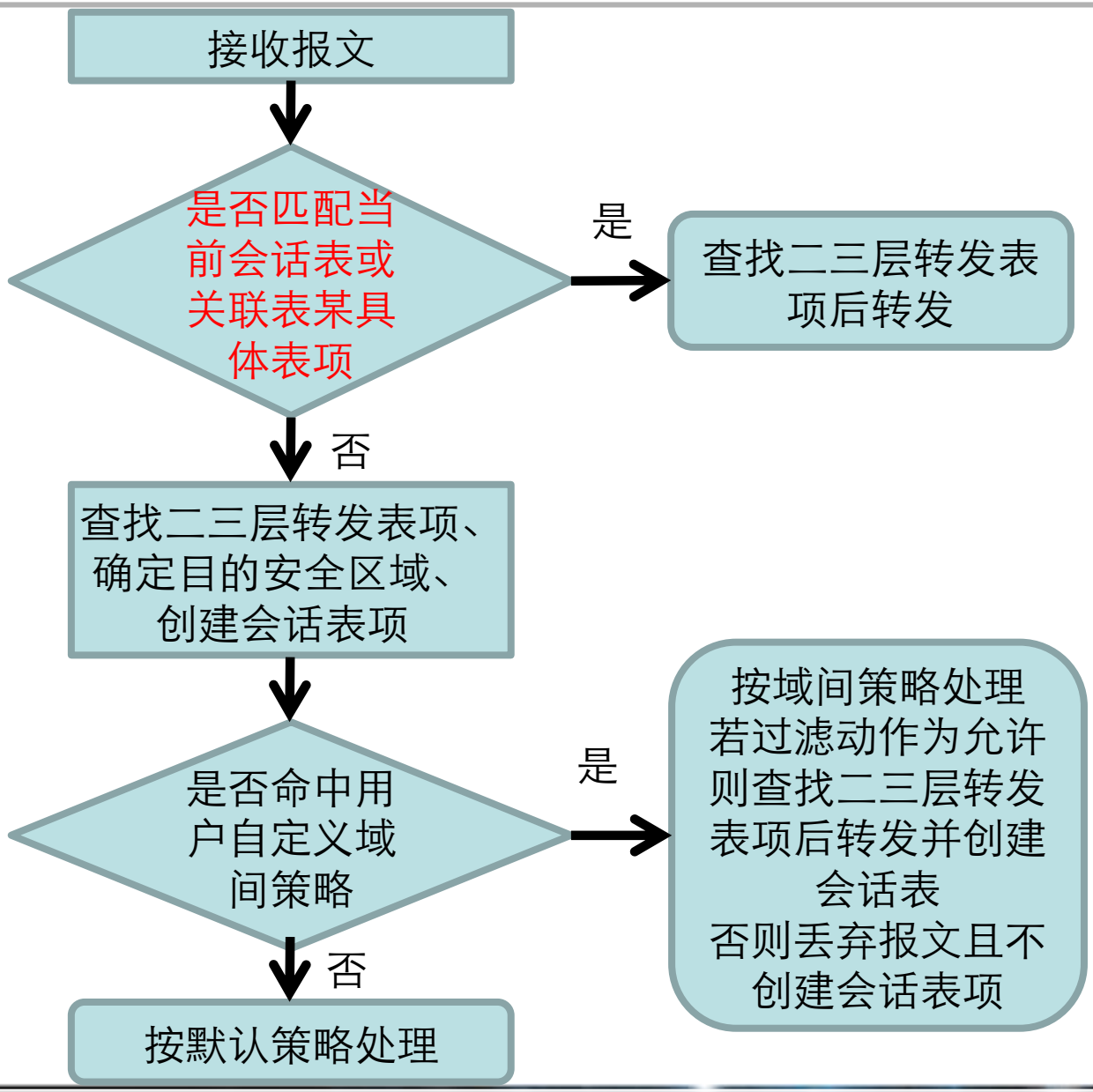
会话关联表概述

- 相对于域间策略，关联表可以理解为防火墙的临时性规则，是基于应用协议动态协商的
- 会话关联表的主要作用：
  - → 动态协商多通道协议的跟踪及数据报文匹配
  - → 应用层网关NAT转换信息记录
  - → 应用协议识别
  - → 父子会话关联

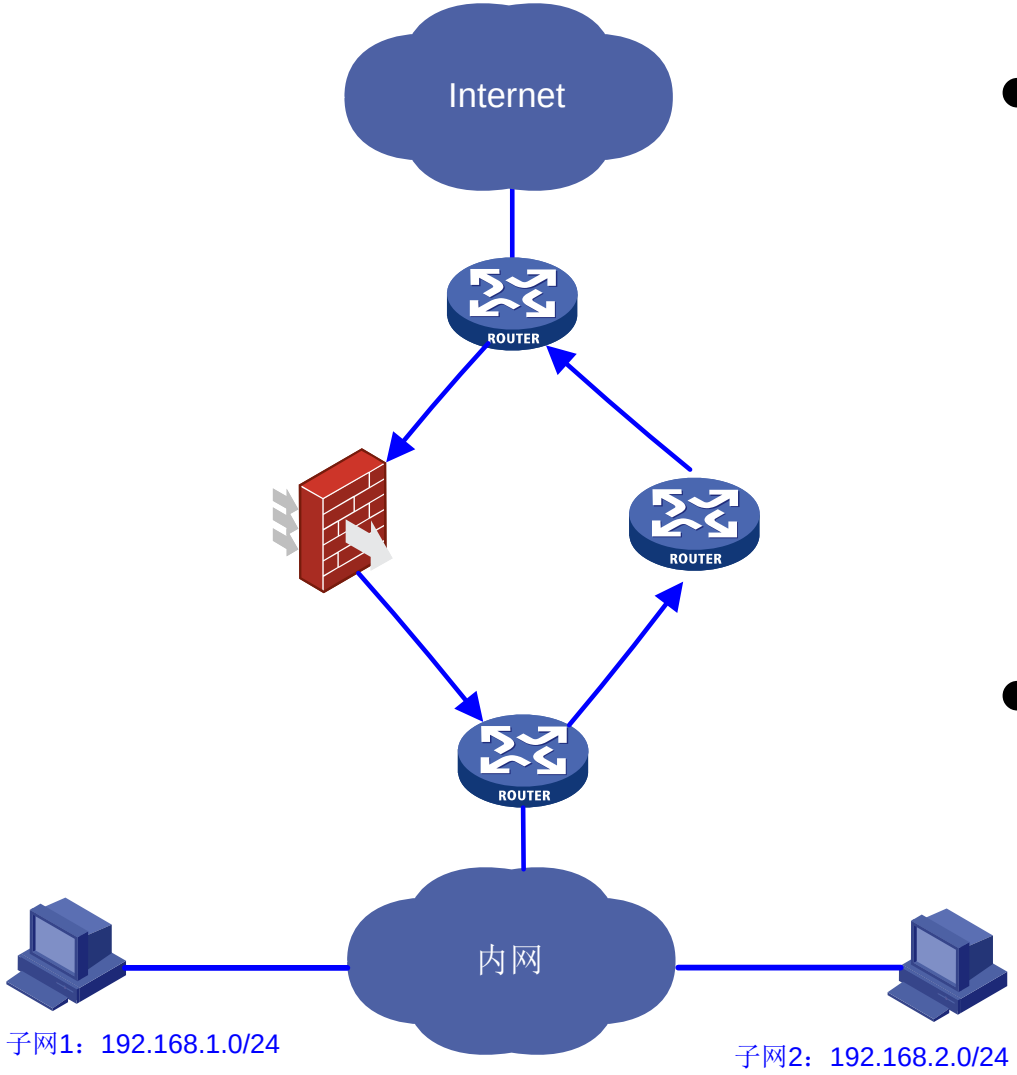
会话关联表相关特性

- 关联表由ALG协调会话管理模块创建。当ALG解析出应用协议报文数据载荷中携带的地址、端口信息后，调用会话管理模块创建关联表(如有NAT则先进行相应的地址、端口转后，然后再创建表项)
- 未配置NAT、LB、域间策略时不会创建关联表
- 关联表是一个三元组表项，使用IP地址、端口、和协议作为Key
- AllowConn表示允许通过关联表创建的子通道个数，如子通道数到达上限则删除关联表。例如FTP关联表，允许子通道数为1，一旦数据连接建立，关联表会立即删除

报文转发流程

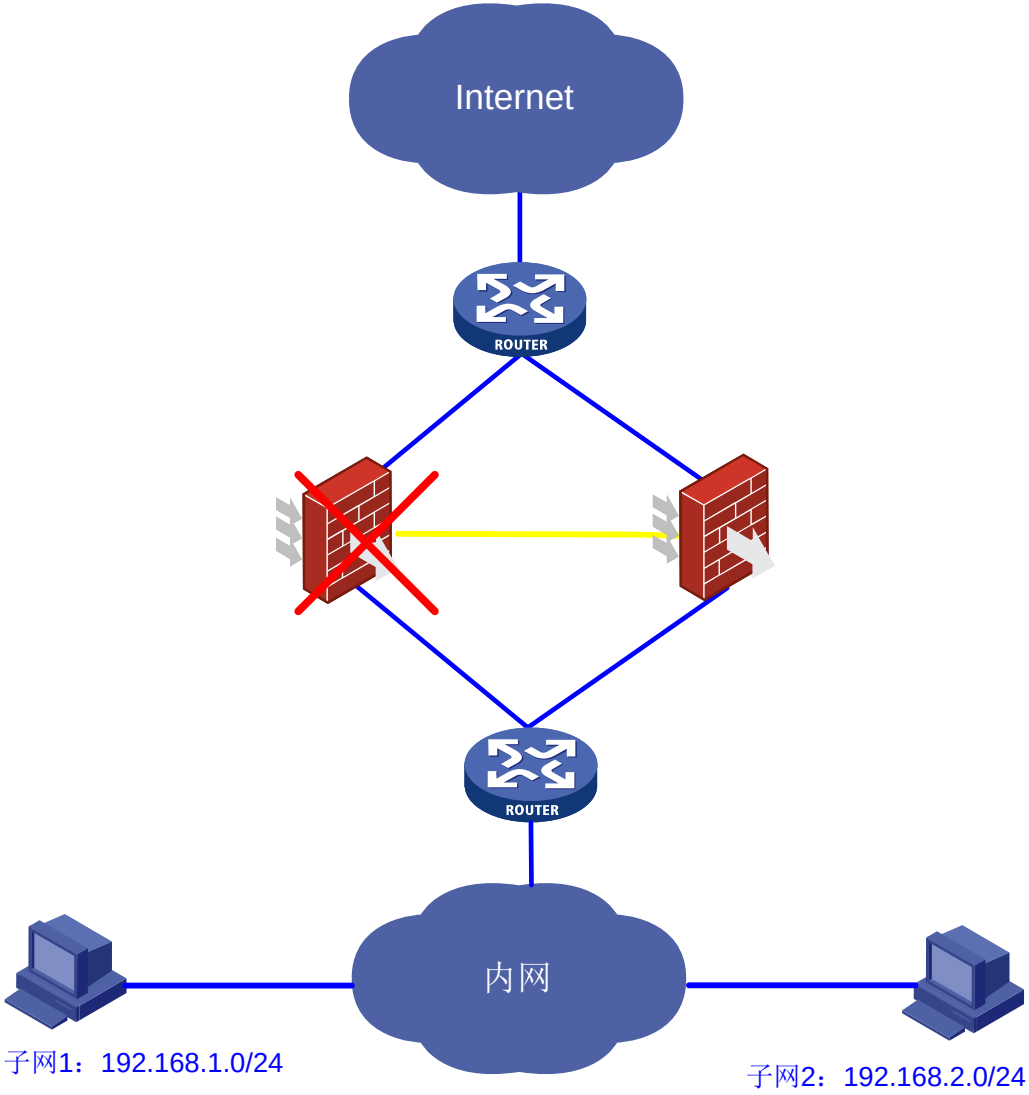

接收报文
是否匹配当前会话表或关联表某具体表项
是
查找二三层转发表项后转发
否
查找二三层转发表项、确定目的安全区域、创建会话表项
是否命中用户自定义域间策略
是
按域间策略处理
若过滤动作为允许
则查找二三层转发表项后转发并创建会话表
否则丢弃报文且不创建会话表项
否
按默认策略处理

单向流检测



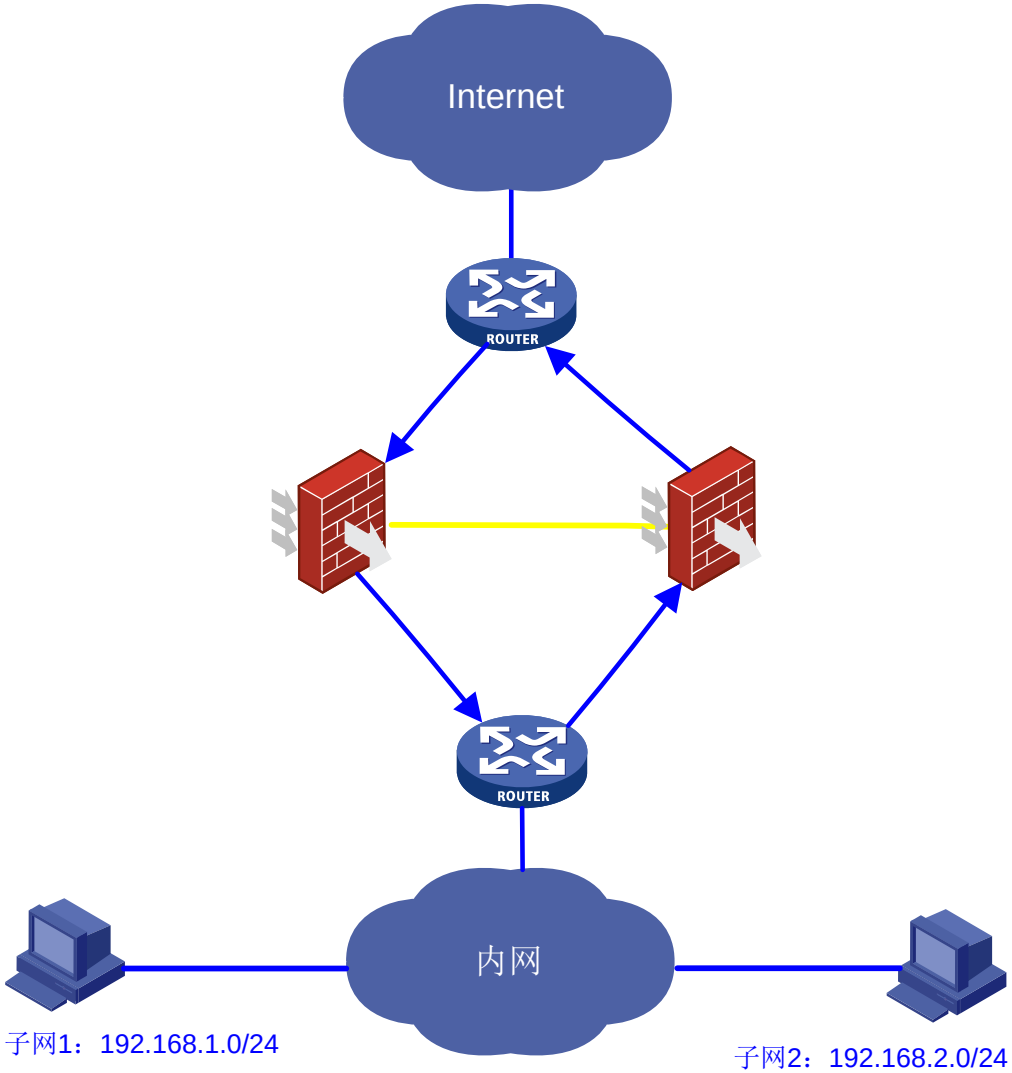
- 单向流量经防火墙处理时必须对协议状态机进行“补充”，在仅能接收单向报文的情况下也可创建稳态会话表项
- 以TCP协议为例：
  - → 允许收到一个方向的syn+ack，或者syn-ack报文之后将会话切换到establish状态
  - → 允许收到一个方向的fin报文之后将会话切换到close状态

会话的双机热备



- 不区分主备状态，两台设备可以同时处理各自的业务报文
- 当会话状态进入TCP-ESTABLISH、UDP-READY和RAWIP-READY状态时对会话表项进行备份
- 可以避免流量在双机切换时出现业务中断

双机热备——非对称路径



- 在会话创建即开始备份
- 在会话状态更新时触发备份
- 对于TCP的Syn-ack、Ack报文和ICMP Reply报文如果在当前设备找不到会话要透传到另一台设备上进行处理

目录

- 会话管理特性基础及实现原理
- 会话管理典型组网及典型配置
- 会话管理常见问题及注意事项

会话表项老化时间基本配置

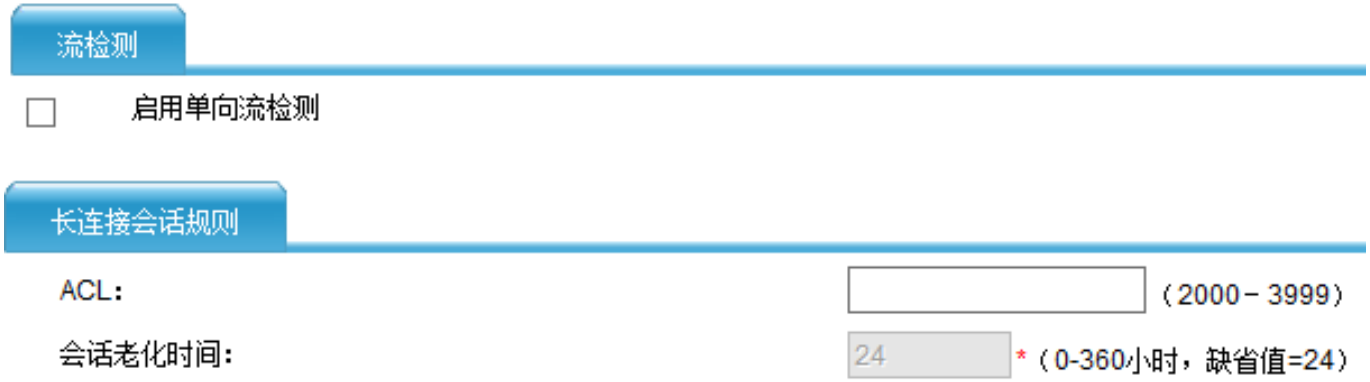
H3C

会话层协议老化时间

TCP协议		
SYN_SENT和SYN_RCV状态老化时间：	30	*（5-100000秒，缺省值=30）
FIN_WAIT状态老化时间：	30	*（5-100000秒，缺省值=30）
ESTABLISHED状态老化时间：	3600	*（5-100000秒，缺省值=3600）
UDP协议		
OPEN状态老化时间：	30	*（5-100000秒，缺省值=30）
READY状态老化时间：	60	*（5-100000秒，缺省值=60）
ICMP协议		
OPEN状态老化时间：	60	*（5-100000秒，缺省值=60）
CLOSED状态老化时间：	30	*（5-100000秒，缺省值=30）
超时加速队列		
超时加速队列老化时间：	10	*（5-100000秒，缺省值=10）
RAWIP协议		
OPEN状态老化时间：	30	*（5-100000秒，缺省值=30）
READY状态老化时间：	60	*（5-100000秒，缺省值=60）

- 配置各协议状态会话老化时间，参数修改后仅对新建会话有效

单向流检测与长连接配置



配置项	说明
启用单向流检测	设置是否启用单向流检测 ●启用单向流检测时，会话管理同时处理单向流和双向流 ●不启用单向流检测时，会话管理仅处理双向流
ACL	根据ACL ID设置长连接会话规则 长连接会话规则同时引用的ACL只能有一个，新设置的ACL会覆盖旧的ACL，不输入ACL ID表示删除长连接会话 注意：ACL规则应匹配会话发起方五元组及相关信息
会话老化时间	设置长连接会话的老化时间 “0”表示长连接会话永不老化

会话双机热备配置

配置项	说明
使能双机热备功能	设置使能或禁止设备的双机热备功能
使能会话双机热备功能	设置使能或禁止会话双机热备功能
支持非对称路径备份	设置会话双机热备是否支持非对称路径备份 • 不支持非对称路径备份：是指两台设备同时正常工作时，一条会话中的数据流进入内网和从内网出去所经过的设备必须相同，即进入内网时经过双机热备中的一台设备，从内网出去时经过的设备是进入时经过的设备 • 支持非对称路径备份：是指两台设备同时正常工作时，一条会话中的数据流进入内网和从内网出去所经过的设备可以不同，即进入内网时经过双机热备中的一台设备，从内网出去时经过的设备可以是进入时经过的设备，也可以是另一台设备 此设置在双机热备的两台设备上必须一致。双机配置同步功能支持此设置的同步

目录

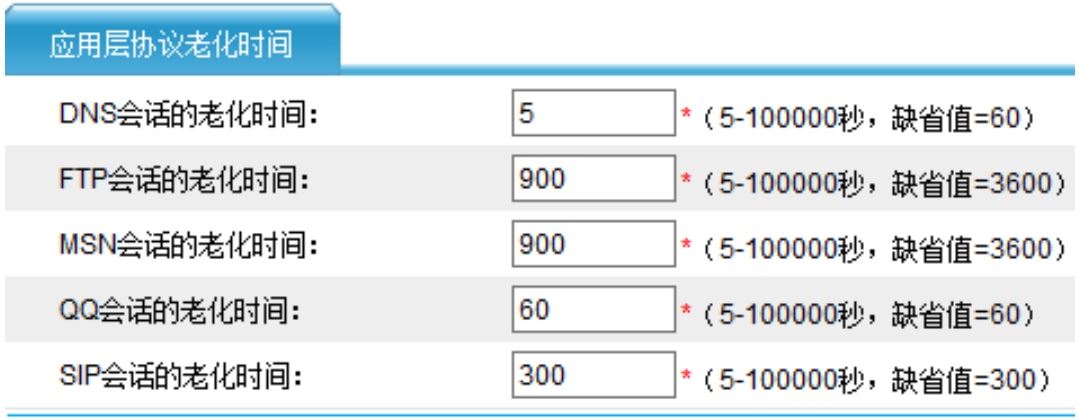
- 会话管理特性基础及实现原理
- 会话管理典型组网及典型配置
- 会话管理常见问题及注意事项

Q：关于会话表项中会话层协议老化时间设置是否有推荐值？

A：会话表项的老化时间设置在大多数设置部署场景中保持默认值即可。在个别部署场景中，设备上的实时并发连接持续较高、甚至接近最大并发连接数时，可以通过适当减小老化时间，以达到降低并发连接数的目的，但切勿设置过短的老化时间。

Q：关于会话表项中应用层协议老化时间设置是否有推荐值？

A：会话表项的应用层协议老化时间设置在大多数设置部署场景中保持默认值即可。在个别部署场景中，当设备上处理的业务流量以DNS业务为主时，可以适当减小DNS会话老化时间以减少设备实时并发连接数。在启用了ALG DNS的情况下，可以调整为5秒。



FAQ

Q：会话长连接有什么应用场景

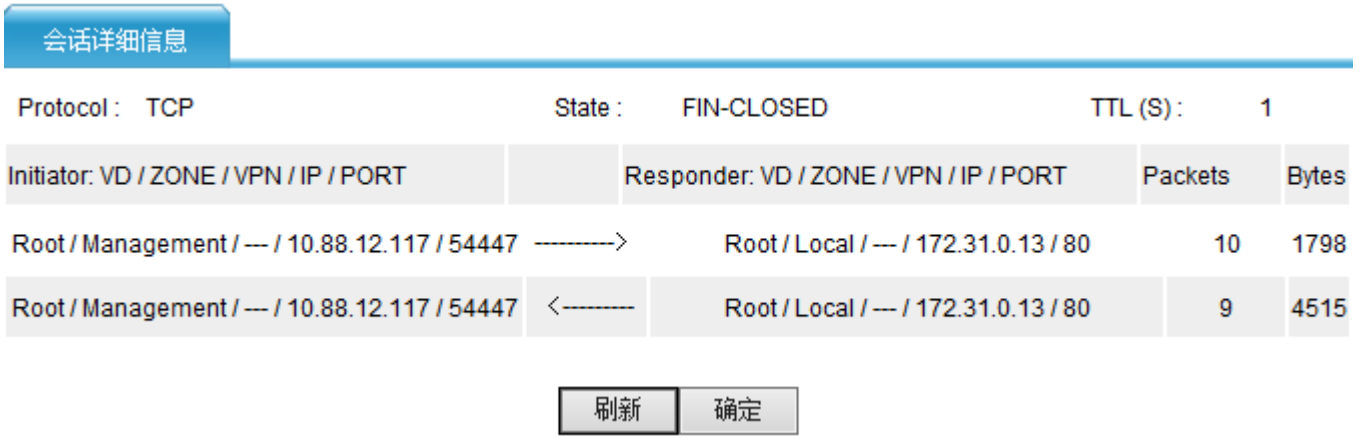
A：会话长连接仅对由TCP承载的应用有效。部分应用层软件在TCP连接建立并进入ESTABLISHED状态后，存在长时间无任何数据传输且不发送TCP保活报文的情形。配置长连接可以避免防火墙在TCP EST老化时间到期后，主动删除对应会话表项致使连接中断的问题。须注意配置长连接时必须使用ACL精确限定发起方五元组，避免设备上建立大量长时间不老化的连接。

Q：启用单向流检测对设备是否有影响

A：启用单向流检测后，部分业务功能将无法支持（如ASPF将无法支持非SYN的TCP首包检查等），系统安全性将会降低。请根据网络环境决定是否启用单向流检测，如果网络中有单向流存在，则应启用单向流检测，否则将无法正确处理单向流；如果网络中没有单向流存在，则应关闭单向流检测，以免影响系统的安全性。

Q：如何查看会话表项相关的详细信息

A： 在设备Web页面的“防火墙－会话管理－会话列表”中，根据条件筛选出需要查看的会话表项后，可以通过单击“查看会话详细信息”按键（放大镜）查看；在命令行中，可以通过携带verbose参数的display session table命令查看会话详细信息。



Q：如何查看会话表统计信息

A：在设备Web页面的“防火墙－会话管理－会话统计”中，可以查看“全局统计信息”等会话相关统计数据；在命令行中，可以display session table命令查看会话详细信息。

全局统计信息 | 历史统计信息 | IP统计信息 | 安全区域统计信息 | 会话统计设置

统计项	统计值
当前总会话数	2
当前TCP连接数	2
当前TCP半开连接数	0
当前TCP半闭连接数	0
当前UDP连接数	0
当前ICMP连接数	0
当前RAWIP连接数	0
当前关联表个数	0
会话创建的速率	0
TCP会话创建的速率	0
UDP会话创建的速率	0
ICMP会话创建的速率	0
RAWIP会话创建的速率	0
当前收到的TCP报文数	13288
当前收到的TCP报文字节数	3537210
当前收到的UDP报文数	0
当前收到的UDP报文字节数	0
当前收到的ICMP报文数	0
当前收到的ICMP报文字节数	0
当前收到的RAWIP报文数	0
当前收到的RAWIP报文字节数	0

本章总结

- 会话管理技术概述及实现原理
- 会话管理典型配置和应用场景
- 会话管理常见问题和注意事项

ITоIP解决方案专家

杭州华三通信技术有限公司

www.h3c.com