目 录

1 会话管理


说明

仅 WX2500H-WiNet 系列不支持 slot 参数。

1.1 会话管理简介

会话管理是为了实现 NAT（Network Address Translation，网络地址转换）、ASPF（Advanced Stateful Packet Filter，高级状态包过滤）、攻击检测及防范等基于会话进行处理的业务而抽象出来的公共功能。此功能把传输层报文之间的交互关系抽象为会话，并根据发起方和响应方的报文信息对会话进行状态更新和老化，支持多个业务特性分别对同一个业务报文进行处理。

会话管理实现的主要功能包括：

- 报文到会话的快速匹配；
- 传输层协议状态的管理；
- 报文应用层协议类型的识别；
- 按照协议状态或应用层协议类型对会话进行老化；
- 支持指定的会话维持较为长时间的连接；
- 为需要进行端口协商的应用层协议提供特殊的报文匹配；
- 支持对 ICMP/ICMPv6 差错控制报文的解析以及根据解析结果进行会话的匹配。

1.1.1 会话管理的工作原理

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来对连接的状态进行跟踪，并对所有连接的状态信息进行基于会话表和关联表的统一维护和管理。

客户端向服务器发起连接请求报文的时候，系统会创建一个会话表项。该表项中记录了一个会话所对应的请求报文信息和回应报文信息，包括源 IP 地址/端口号、目的 IP 地址/端口号、传输层协议类型、应用层协议类型、会话的协议状态等。对于多通道协议（特指部分应用协议中，客户端与服务器之间需要在已有连接基础上协商新的连接来完成一个应用），会话管理还会根据协议的协商情况，创建一个或多个（由具体的应用协议决定）关联表表项，用于关联属于同一个应用的不同会话。关联表项在多通道协议协商的过程中创建，完成对多通道协议的支持后即被删除。

上述会话管理的工作原理描述仅针对目的地址为单播地址的报文，对于目的地址是组播地址的报文稍有不同。组播报文到达设备后通常经由一个入接口到多个出接口进行转发，因此对于同一个应用的组播报文的连接，在入接口和多个出接口均会建立起各自的会话表项，我们称这类组播报文触发建立的会话表项为组播会话表项，以区别于单播报文触发建立的单播会话表项。若无特殊说明，本文中的会话表项不区分单播和组播类型。

在实际应用中，会话管理作为公共功能，只能实现连接状态的跟踪，并不能阻止潜在的攻击报文通过。会话管理配合 ASPF 特性，可实现根据连接状态信息动态地决定是否允许数据包通过防火墙进入内部区域，以便阻止恶意的入侵。

1.1.2 会话管理在设备上的实现

目前会话管理在设备上实现的具体功能如下：

- 支持对各协议报文创建会话、更新会话状态以及根据协议状态设置老化时间。
- 支持 ICMP/ICMPv6 差错报文的映射，可以根据 ICMP/ICMPv6 差错报文携带的信息查找原始的会话。
- 支持设置长连接会话，保证指定的会话在一段较长的时间内不会被老化。
- 支持应用层协议（如 FTP）的控制通道和动态数据通道的会话管理。

1.2 配置会话管理

会话管理支持的配置包括：协议状态的会话老化时间、长连接会话规则及删除会话。这些配置可根据实际应用需求选择进行，配置无先后顺序的要求，相互不关联。

长连接老化时间仅在 TCP 会话进入稳态（TCP-EST 状态）时生效。在会话稳态时，长连接老化时间具有最高的优先级，其次为协议状态老化时间。

1.2.1 配置协议状态会话老化时间

提示

当会话数目过多时（大于 80 万条），建议不要将协议状态老化时间设置得过短，否则会造成设备响应速度过慢。

以下配置用于实现根据会话所处协议状态来设置会话表项的老化时间。处于某协议状态的会话，如果在该协议状态老化时间内未被任何报文匹配，则会由于老化而被系统自动删除。

表1-1 配置各协议状态的会话老化时间

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置各协议状态的会话老化时间	**session aging-time state** { **fin** | **icmp-reply** | **icmp-request** | **rawip-open** | **rawip-ready** | **syn** | **tcp-close** | **tcp-est** | **tcp-time-wait** | **udp-open** | **udp-ready** } *time-value*	缺省情况下，各协议状态的会话老化时间为： • FIN：30 秒 • ICMP-REPLAY：30 秒 • ICMP-REQUEST：60 秒 • RAWIP-OPEN：30 秒 • RAWIP-READY：60 秒 • SYN：30 秒 • TCP-CLOSE：2 秒 • TCP-EST：3600 秒 • TCP-TIME-WAIT：2 秒 • UDP-OPEN：30 秒 • UDP-READY：60 秒

1.2.2 配置长连接会话规则

针对进入 TCP-EST 状态的 TCP 会话，用户可以根据需要将符合指定特征的 TCP 会话设置为长连接会话。长连接会话的老化时间不会随着状态的变迁而更改，可以将其设置得比普通会话的老化时间更长，或者设置成永不老化。被设置成永不老化的长连接会话，只有当会话的发起方或响应方主动发起关闭连接请求或管理员手动删除该会话时，才会被删除。

系统支持配置多条长连接会话规则。

表1-2 配置长连接会话规则

操作	命令	说明
进入系统视图	**system-view**	-
配置长连接会话规则	**session persistent acl** [**ipv6**] *acl-number* [**aging-time** *time-value*]	缺省情况下，无长连接会话规则

1.2.3 开启会话统计功能

开启会话统计功能之后，设备将对收到和发送的基于会话的业务报文数目和报文字节数进行统计。基于单播会话的报文统计信息可通过 **display session table** 命令查看，基于单播报文类型的报文统计信息可通过 **display session statistics** 命令查看；基于组播会话的报文统计信息可通过 **display session table multicast** 命令查看，基于组播报文类型的报文统计信息可通过 **display session statistics multicast** 命令查看。

表1-3 配置会话统计

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
开启会话统计功能	**session statistics enable**	缺省情况下，会话统计功能处于关闭状态

1.2.4 配置会话状态机为宽松模式

在非对称路径网络中，若设备上未开启会话业务热备份功能，则需要将会话状态机的模式配置为宽松模式，可以避免设备异常丢包。

在对称路径网络中，建议保持缺省状态，即严格模式。

表1-4 配置会话状态机为宽松模式

操作	命令	说明
进入系统视图	**system-view**	-
配置会话状态机为宽松模式	**session state-machine mode loose**	缺省情况下，会话状态机为严格模式

1.3 配置会话日志

会话日志是为满足网络管理员安全审计的需要，对用户的访问信息、用户 IP 地址的转换信息、用户的网络流量信息等进行记录，并可采用日志的格式发送给日志主机或者输出到信息中心。

存活时间或收发数目达到一定阈值的会话才会以日志的形式进行记录并输出，该阈值包括以下两种类型：

- 时间阈值：当一个会话存在的时间达到设定的时间阈值时，输出会话日志。
- 流量阈值：分为报文数阈值和字节数阈值两种。当一个会话收发的报文数或字节数达到设定的流量阈值时，输出会话日志。为使流量阈值能触发输出会话日志，必须开启会话统计功能；否则，会话会由于无法统计报文的流量信息而不能通过流量阈值触发输出会话日志。

同时配置了时间阈值和流量阈值的情况下，只要有一个阈值到达，就会输出相应的会话日志，并将所有的阈值统计信息清零。

同时只能有一种流量阈值有效，以最后一次配置的阈值类型为准，例如，先配置报文数阈值再配置字节数阈值，则当前有效的阈值是字节数阈值，只会输出达到字节数阈值的会话日志。

开启会话日志功能后，若开启了新建会话日志功能和删除会话日志功能，则在会话表创建和删除时分别输出一次会话日志；否则在会话表创建和删除时不会输出会话日志。

需要注意的是：会话日志功能和 Flow 日志功能的相关配置必须同时配置后才能生成会话日志信息。有关 Flow 日志模块的相关配置请参见“网络管理和监控配置指导”中的“Flow 日志”。

表1-5 配置会话日志功能

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置输出会话日志的时间阈值	**session log time-active** *time-value*	缺省情况下，未配置输出会话日志的时间阈值

操作	命令	说明
（可选）配置输出会话日志的流量阈值	**session log** { **bytes-active** *bytes-value* | **packets-active** *packets-value* }	缺省情况下，未配置输出会话日志的流量阈值
（可选）开启新建会话日志功能	**session log flow-begin**	缺省情况下，新建会话日志功能处于关闭状态
（可选）开启删除会话日志功能	**session log flow-end**	缺省情况下，删除会话日志功能处于关闭状态
进入接口视图	**interface** *interface-type interface-number*	-
开启会话日志功能	**session log enable** { **ipv4** | **ipv6** } [**acl** *acl-number*] { **inbound** | **outbound** }	缺省情况下，会话日志功能处于关闭状态

说明

session log time-active、**session log** { **bytes-active** *bytes-value* | **packets-active** *packets-value* }、**session log flow-begin** 和 **session log flow-end** 以上命令至少选其一。

1.4 会话管理显示和维护

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会话的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除会话统计信息。

表1-6 会话管理显示和维护

操作	命令
显示各协议状态的会话老化时间	**display session aging-time state**
显示IPv4单播会话表信息	**display session table ipv4** [**slot** *slot-number*] [**source-ip** *start-source-ip* [*end-source-ip*]] [**destination-ip** *start-destination-ip* [*end-destination-ip*]] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**verbose**]
显示IPv6单播会话表信息	**display session table ipv6** [**slot** *slot-number*] [**source-ip** *start-source-ip* [*end-source-ip*]] [**destination-ip** *start-destination-ip* [*end-destination-ip*]] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**verbose**]
根据五元组显示IPv4单播会话统计信息	**display session statistics ipv4** { **source-ip** *source-ip* | **destination-ip** *destination-ip* | **protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** } | **source-port** *source-port* | **destination-port** *destination-port* } * [**slot** *slot-number* [**cpu** *cpu-number*]]
根据五元组显示IPv6单播会话统计信息	**display session statistics ipv6** { **source-ip** *source-ip* | **destination-ip** *destination-ip* | **protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** } | **source-port** *source-port* | **destination-port** *destination-port* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

操作	命令
显示单播会话统计信息	**display session statistics** [**summary**] [**slot** *slot-number*]
显示IPv4组播会话表信息	**display session table multicast ipv4** [**slot** *slot-number*] [**source-ip** *start-source-ip* [*end-source-ip*]] [**destination-ip** *start-destination-ip* [*end-destination-ip*]] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**verbose**]
显示IPv6组播会话表信息	**display session table multicast ipv6** [**slot** *slot-number*] [**source-ip** *start-source-ip* [*end-source-ip*]] [**destination-ip** *start-destination-ip* [*end-destination-ip*]] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**verbose**]
显示组播会话统计信息	**display session statistics multicast** [**slot** *slot-number*]
显示关联表信息	**display session relation-table** { **ipv4** | **ipv6** } [**slot** *slot-number*]
删除IPv4单播会话表项	**reset session table ipv4** [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*]
删除IPv6单播会话表项	**reset session table ipv6** [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*]
删除所有单播会话项	**reset session table** [**slot** *slot-number*]
清除单播会话统计信息	**reset session statistics** [**slot** *slot-number*]
删除IPv4组播会话表项	**reset session table multicast ipv4** [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*]
删除IPv6组播会话表项	**reset session table multicast ipv6** [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*]
删除所有组播会话项	**reset session table multicast** [**slot** *slot-number*]
清除组播会话统计信息	**reset session statistics multicast** [**slot** *slot-number*]
删除关联表项	**reset session relation-table** [**ipv4** | **ipv6**] [**slot** *slot-number*]