H3C SecPath 系列防火墙

服务链配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W206-20191125
产品版本：

F5030/F5030-6GW/F5060/F5080/F5000-M	R9606
F5010/F5020/F5040/F5000-S/F5000-C	R9320
F1005/F1010/F1000-AK108/AK109/AK110/AK115/AK120/AK125/AK710	R9514
F1020/F1030/F1050/F1060/F1070/F1080/F1070-GM/F1000-AK130/AK135/AK140/AK145/AK150/AK155/AK160/AK165/AK170/AK175/AK180/AK185/AK711/F1000-GM-AK370/F1000-GM-AK380	R9323
LSU3FWCEA0/LSUM1FWCEAB0/LSX1FWCEA1	R8219
LSPM6FWD	R8513
LSXM1FWDF1/LSUM1FWDEC0/IM-NGFWX-IV/LSQM1FWDSC0/LSWM1FWD0	R8514

前 言

本配置指导介绍了防火墙产品各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《服务链配置指导》主要介绍服务链相关的特性。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 服务链

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	服务链	支持
F1005/F1010/F1020/F1030/F1050/F1060/F1070/F1080/F1070-GM		不支持
F1000-AK108/AK109/AK110/AK115/AK120/AK125/AK130/AK135/AK140/AK145/AK150/AK155/AK160/AK165/AK170/AK175/AK180/AK185/AK710/AK711		不支持
F1000-GM-AK370/F1000-GM-AK380		不支持
LSU3FWCEA0/LSUM1FWCEAB0/LSX1FWCEA1		不支持
LSXM1FWDF1/LSUM1FWDEC0/IM-NGFWX-IV/LSQM1FWDSC0/LSWM1FWD0/LSPM6FWD		• LSUM1FWDEC0/IM-NGFWX-IV/LSQM1FWDSC0/LSPM6FWD：不支持 • LSXM1FWDF1/LSWM1FWD0：支持

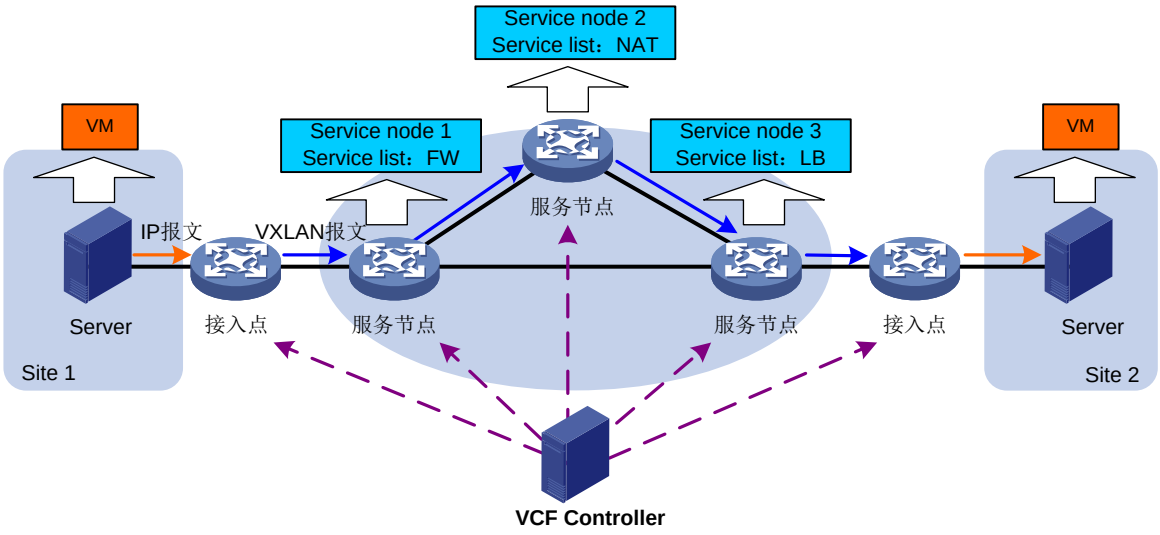
1.1 服务链简介

服务链（Service Chain）技术应用于 VXLAN 网络，它结合 SDN（Software Defined Network，软件定义网络）来实现业务编排，引导网络业务报文按照要求的顺序通过服务节点进行处理和转发。

1.1.1 典型组网

如图 1-1 示，VCFC（VCF Controller，VCF 控制器）基于不同的租户应用，通过 OpenFlow 下发引流规则来控制 Overlay 网络中的 VXLAN 报文是否进入服务链处理，并确保报文在服务链内各个节点间传递。

图1-1 服务链应用示意图



1.1.2 服务节点角色

服务链分为接入点和服务节点两种角色。

1. 接入点

接入点是 VXLAN 网络的边缘设备 VTEP（VXLAN Tunnel End Point，VXLAN 隧道端点）。由它根据 VCFC 下发的引流规则对报文进行 VXLAN 封装，并填充服务链信息。

2. 服务节点

服务节点是网络中处理某种业务的设备，可以是物理设备，也可以是 NFV（Network Function Virtualisation，网络功能虚拟化）设备。一条服务链上可以存在多个服务节点。各服务节点根据服务列表指定的服务类型对报文进行处理。

服务列表用于指定服务的类型及处理顺序，目前仅支持 FW、和 LB 两种服务类型。

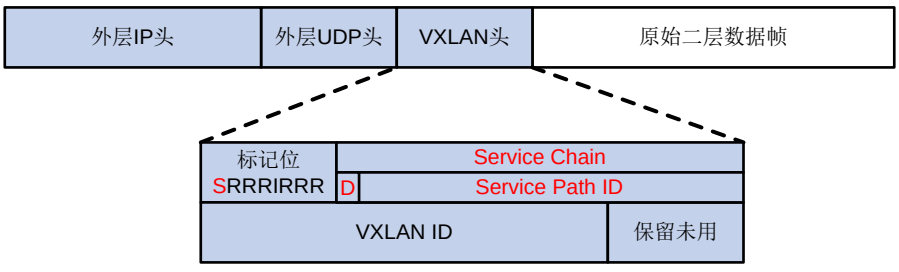
服务节点包含两种特殊的节点类型：

- 首节点：服务链中首个对报文进行处理的服务节点。
- 尾节点：服务链中最后一个对报文进行处理的服务节点。

1.1.3 报文格式

服务链报文采用 VXLAN 封装，并在 VXLAN 报文头中标识服务链信息，如图 1-2 所示。

图1-2 携带服务链信息的 VXLAN 报文格式示意图



在 VXLAN 报文头中，以下两个字段用于标识报文所使用的服务链：

- 标记位：“S”位为 1 时，表示 VXLAN 头中的 Service Chain 字段有效；为 0，表示 Service Chain 字段无效。
- Service Chain：长度为 24 比特，由方向标记位 D 和 Service Path ID 两部分组成。“D”位为 0 时，表示正向报文；为 1 时，表示反向报文。Service Path ID 长度为 23 比特，用来标识一个服务链。

1.1.4 工作原理

服务链的工作原理大致如下：

(1) 报文入方向的接入点根据 VCFC 下发的引流规则将报文进行 VXLAN 封装，然后发送给服务链的首节点。

(2) 服务链的首节点收到 VXLAN 报文后，根据报文头中的 Service Path ID 字段在本地查找匹配的服务链。

- 如果本地没有匹配的服务链，则该报文进行正常的 VXLAN 转发。
- 如果本地存在匹配的服务链，则该报文进入服务链处理。

(3) 服务链完成处理后：

- 如果该服务链配置了下一跳地址，则报文转发给下一个服务节点处理。
- 如果该服务链没有配置下一跳地址，则该节点作为服务链的尾节点，删除 VXLAN 报文中的 Service Path ID 字段，并将报文转发给报文出方向的接入点。

(4) 报文出方向的接入点对 VXLAN 报文进行解封装，并进行 IP 转发。

1.1.5 服务链配置方式介绍

服务链可以通过 VCFC 和命令行两种方式进行配置，建议采用 VCFC 通过 NETCONF 下发配置的方式。本手册仅介绍命令行的配置方式，通过 VCFC 配置的详细介绍请参见 VCFC 配套的手册。

当设备作为接入点时，只能通过 VCFC 进行配置

1.2 配置服务节点

当设备作为服务节点时，需要进行以下配置：

(1) 创建服务链，并指定正向报文的下一个服务节点及反向报文的下一个服务节点。需要注意的是：

- 如果设备作为服务链的首节点，则仅需要为其指定正向报文的下一个服务节点即可。
- 如果设备作为服务链的尾节点，则仅需要为其指定反向报文的下一个服务节点即可。

(2) 创建服务节点并配置服务节点处理的业务类型。

表1-1 配置服务节点

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建服务链，并进入服务链视图	**service-chain path** *path-id*	缺省情况下，不存在服务链
配置正向报文下一个服务节点的IP地址	**next-service-node** *ip-address*	缺省情况下，未配置正向报文下一个服务节点的IP地址
配置反向报文下一个服务节点的IP地址	**previous-service-node** *ip-address*	缺省情况下，未配置反向报文下一个服务节点的IP地址
创建服务节点，并进入服务节点视图	**service function** *function-id*	缺省情况下，不存在服务节点
配置服务列表	**service list** { **fw** | **lb** }*	缺省情况下，不存在服务列表

1.3 服务链显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示服务链的配置情况，通过查看显示信息验证配置的效果。

表1-2 服务链显示和维护

操作	命令
显示服务链信息	**display service-chain path** { *path-id* | **all** }
显示服务链的统计信息	**display service-chain statistics**