

H3C SecPath 入侵防御系统

VPN 实例配置指导(V7)

新华三技术有限公司

<http://www.h3c.com>

资料版本：6W204-20190429

产品版本：

T5010/T5020

R8514

T5030/T5060/T5080/T5000-S/T5000-C

R8501

T1020/T1030/T1050/T1060/T1080

R8514

T1000-AK340/AK350

R8514

LSWM1IPSD0/LSQM1IPSDSC0/IM-IPSX-IV

R8512

Copyright © 2017-2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本配置指导主要介绍 VPN 实例配置。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 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择一个或者不选。
{ 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择一个、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 VPN实例.....	1-1
1.1 VPN实例基本概念	1-1
1.2 配置VPN实例	1-1
1.2.1 创建VPN实例.....	1-1
1.2.2 配置VPN实例与接口关联.....	1-1
1.3 VPN实例显示和维护	1-2

1 VPN实例

1.1 VPN实例基本概念

1. Site

Site（站点）的含义可以从下述几个方面理解：

- Site 是指相互之间具备 IP 连通性的一组 IP 系统，并且这组 IP 系统的 IP 连通性不需通过服务提供商网络实现；
- Site 的划分是根据设备的拓扑关系，而不是地理位置，尽管在大多数情况下一个 Site 中的设备地理位置相邻；
- 一个 Site 中的设备可以属于多个 VPN，换言之，一个 Site 可以属于多个 VPN；

对于多个连接到同一服务提供商网络的 Site，通过制定策略，可以将它们划分为不同的集合（set），只有属于相同集合的 Sites 之间才能通过服务提供商网络互访，这种集合就是 VPN。

2. VPN实例

在 L3VPN 中，不同 VPN 之间的路由隔离通过 VPN 实例（VPN-instance）实现，VPN 实例又称为 VRF（Virtual Routing and Forwarding，虚拟路由和转发）实例。

1.2 配置VPN实例

1.2.1 创建VPN实例

VPN 实例在实现中与 Site 关联。VPN 实例不是直接对应于 VPN，一个 VPN 实例综合了和它所对应 Site 的 VPN 成员关系和路由规则。

表1-1 创建 VPN 实例

操作	命令	说明
进入系统视图	system-view	-
创建VPN实例，并进入VPN实例视图	ip vpn-instance <i>vpn-instance-name</i>	缺省情况下，不存在VPN实例
（可选）配置VPN实例的描述信息	description <i>text</i>	缺省情况下，未配置VPN实例的描述信息

1.2.2 配置VPN实例与接口关联



提示

执行 **ip binding vpn-instance** 命令将删除接口上已经配置的 IP 地址，因此需要重新配置接口的 IP 地址。

表1-2 配置 VPN 实例与接口关联

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type interface-number</i>	-
配置接口与指定VPN实例关联	ip binding vpn-instance <i>vpn-instance-name</i>	缺省情况下，接口未关联VPN实例，接口属于公网

1.3 VPN实例显示和维护

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的运行情况，通过查看显示信息验证配置的效果。

表1-3 VPN 实例显示和维护

操作	命令
显示指定VPN实例信息	display ip vpn-instance [instance-name <i>vpn-instance-name</i>]