目 录

1 加密引擎 1-1
1.1 加密引擎简介 1-1
1.2 配置硬件加密引擎 1-1
1.3 加密引擎显示和维护 1-2

1 加密引擎

1.1 加密引擎简介

加密引擎是专门用于提供数据加/解密服务的硬件及软件的统称，具体分为硬件加密引擎和软件加密引擎两种类型。

- 硬件加密引擎是集成在 CPU 上的协处理器或者硬件加密卡，由于使用硬件进行加/解密处理，因此具有加速加密的能力，可以提高设备的处理效率。硬件加密引擎的开关状态可由配置控制；
- 软件加密引擎是设备上所有软件加密算法的集合，通过系统自身的软件算法进行加/解密处理。软件加密引擎一直处于开启状态，不可配。

当硬件加密引擎处于开启状态时，设备优先选择硬件加密引擎执行加/解密功能，若设备不支持硬件加密引擎或者其上的所有硬件加密引擎均不支持业务模块所要求的算法时，设备会选择软件加密引擎执行相应的加/解密功能；当硬件加密引擎处于关闭状态时，设备只能选择软件加密引擎执行加/解密功能。

加密引擎可以为 IPsec 等需要加密的业务模块服务，与业务模块的交互过程是：各业务模块将需要加/解密的数据发送给加密引擎，加密引擎对数据进行加/解密处理，然后加密引擎将处理后的数据发送回各业务模块。

1.2 配置硬件加密引擎

硬件加密引擎默认是开启的，可以通过 **crypto-engine accelerator disable** 命令关闭该功能。关闭硬件加密引擎会严重影响加/解密性能，因此仅允许在测试、调试或故障排除的环境下关闭，正常情况下不建议关闭该功能。

硬件加密引擎的开启或关闭状态的改变对业务模块的影响由业务模块决定，例如，对于 IPsec 业务来说，硬件加密引擎状态的改变只对新建立的 IPsec SA 有影响，已建的 IPsec SA 仍旧使用之前选择的加密引擎来处理。因此，建议在开启或关闭硬件加密引擎之后，使用 **reset ipsec sa** 命令将当前已有的 IPsec SA 删除，使得所有新建立的 IPsec SA 都将使用新选择的加密引擎处理流程来处理。

表1-1 配置硬件加密引擎

操作	命令	说明
进入系统视图	**system-view**	-
关闭硬件加密引擎	**crypto-engine accelerator disable**	缺省情况下，硬件加密引擎处于开启状态
开启硬件加密引擎	**undo crypto-engine accelerator disable**	

1.3 加密引擎显示和维护

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

在用户视图下执行 **reset** 命令可以清除加密引擎的统计信息。

表1-2 加密引擎显示和维护

操作	命令
显示加密引擎的基本信息	**display crypto-engine**
显示加密引擎的统计信息	**display crypto-engine statistics** [**engine-id** *engine-id*]
清除加密引擎的统计计数	**reset crypto-engine statistics** [**engine-id** *engine-id*]