在IPSec中DPD是什么含义?

刘军 2006-10-25 发表

在IPSEC中DPD是什么含义?

IPSec DPD（IPSec Dead Peer Detection on-demand）为按需型IPSec/IKE安全隧道对端状态探测功能。启动DPD功能后，当接收端长时间收不到对端的报文时，能够触发DPD查询，主动向对端发送请求报文，对IKE Peer是否存在进行检测。

与IPSec中原有的周期性Keepalive功能相比，DPD具有产生数据流量小、检测及时、隧道恢复快的优点。

在安全网关与VRRP备份组的虚地址之间建立ISAKMP SA的应用方案中，DPD功能保证了VRRP备份组中主备切换时安全隧道能够迅速自动恢复。解决了VRRP备份组主备切换使安全隧道通信中断的问题，扩展了IPSec的应用范围，提高了IPSec协议的健壮性。

该功能符合RFC3706、RFC2408。

(1) 定时器

IPSec DPD在发送和接收DPD报文中使用了两个定时器：intervaltime和timeout。

- intervaltime：触发DPD查询的间隔时间，该时间指明隔多久没有收到对端IPSec报文时触发DPD查询。
- timeout：等待DPD应答报文超时时间。

(2) 运行机制

- 发送端

当启动了DPD功能以后，如在intervaltime定时器指定的时间间隔内没有收到对端的IPSec报文，且本端欲向对端发送IPSec报文时，DPD向对端发送DPD请求，并等待应答报文。如果超过timeout定时器设定的超时时间仍然未收到正确的应答报文，DPD记录失败事件1次。当失败事件达到3次时，删除ISAKMP SA 和相应的IPSec SA。

对于路由器与VRRP备份组虚地址之间建立的IPSec SA，连续3次失败后，安全隧道同样会被删除，但是当有符合安全策略的报文重新触发安全联盟协商时，会重新建立起安全隧道。切换时间的长短与timeout定时器的设置有关，定时器设定的超时时间越短，通信中断时间越短（注意：超时时间过短会增加网络开销，一般情况下采用缺省值即可）。

- 接收端

收到请求报文后，发送响应报文。