11.5.4 基线的其他注意事项

下面是创建网络基线的一些额外注意事项。

- 创建每个基线都至少要经过 3 次：低流量期间一次（早晨）、高流量期间一次（下午三点左右）、无流量期间一次（深夜）。
- 有可能的话，尽量避免直接在需要创建基线的主机上捕获流量。因为在高流量期间，这可能会增加设备负载和影响性能，并可能因数据包丢失导致基线无效。
- 你的基线可能包含一些与网络有关的私密信息，一定要保护好它。将它存储在安全的地方，只有合适的人才有访问权限。但同时别放得太偏，以免需要时找不到。可以考虑将它存放在 U 盘或者加密分区里。
- 让所有.pcap 文件与你的基线关联，为更常见的参考值写一份「小抄」，比如关联关系或数据传输率。