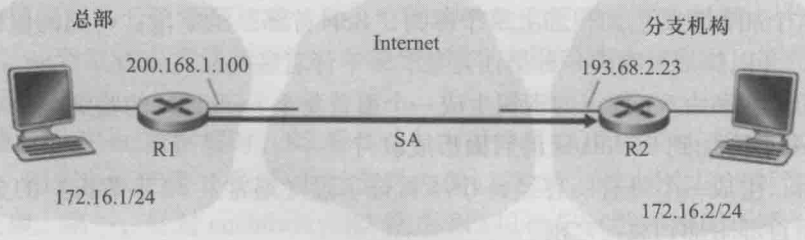

图 8-28 从 R1 到 R2 的安全关联

我们现在观察 SA 的“内部”。为了使讨论明确和具体，我们在图 8-28 中的一个从路由器 R1 到路由器 R2 的 SA 场景下进行观察。（你能够认为路由器 R1 是图 8-27 中的总部网关路由器，而路由器 R2 是图 8-27 中的分支机构网关路由器。）路由器 R1 将维护有关该 SA 的状态信息，这将包括：

- SA 的 32 比特的标识符，称为**安全参数索引**（Security Parameter Index，SPI）。
- SA 的初始接口（在此例中为 200.168.1.100）和 SA 的目的接口（在此例中为 193.68.2.23）。
- 将使用的加密类型（例如，具有 CBC 的 3DES）。
- 加密密钥。
- 完整性检查的类型（例如，具有 MD5 的 HMAC）。
- 鉴别密钥。

无论何时路由器 R1 需要构建一个 IPsec 数据报经过这个 SA 转发，它访问该状态信息以决定它应当如何鉴别和加密该数据报。类似地，路由器 R2 将维护对此 SA 的相同的状态信息，并将使用该信息鉴别和加密任何从该 SA 到达的 IPsec 数据报。

一个 IPsec 实体（路由器或主机）经常维护许多 SA 的状态信息。例如，在图 8-27 中具有 n 个销售员的 VPN 例子中，总部网关路由器维护 $(2+2n)$ 个 SA 的状态信息。一个 IPsec 实体在它的**安全关联数据库**（Security Association Database，SAD）中存储其所有 SA 的状态信息，SAD 是实体操作系统内核中的一个数据结构。

8.7.4 IPsec 数据报

在描述了 SA 后，我们现在能够描述实际的 IPsec 数据报了。IPsec 有两种不同的分组形式，一种用于所谓**隧道模式**（tunnel mode），另一种用于所谓**运输模式**（transport mode）。更为适合 VPN 的隧道模式比运输模式部署得更为广泛。为了进一步讲清 IPsec 和避免许多难题，我们因此专门关注隧道模式。一旦已经牢牢地掌握了隧道模式，应当能够容易地自学运输模式。

IPsec 数据报的分组格式显示在图 8-29 中。你也许认为分组格式是枯燥乏味的，但我们将很快看到 IPsec 数据报实际上尝起来像美式墨西哥风味（Tex-Mex）美食！我们考察图 8-28 的场景中的 IPsec 字段。假设路由器 R1 接收到一个来自主机 172.16.1.17（在总部网络中）的普通 IPv4 数据报，该分组的目的地是主机 172.16.2.48（在分支机构网络中）。路由器 R1 使用下列方法将这个“普通 IPv4 数据报”转换成一个 IPsec 数据报：

- 在初始 IPv4 数据报（它包括初始首部字段！）后面附上一个“ESP 尾部”字段。