IPSEC模式下ESP报文的装包与拆包

IPSEC

“Internet 协议安全性 （**IPSec**）”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 （**IP**） 网络上进行保密而安全的通讯。**IPSec**是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 **IPSec** 保护的计算机。

IPSec由两部分组成：

1. ***IKE协议***：建立安全分组流的密钥交换协议；
2. ***ESP协议***：保护分组流的协议。

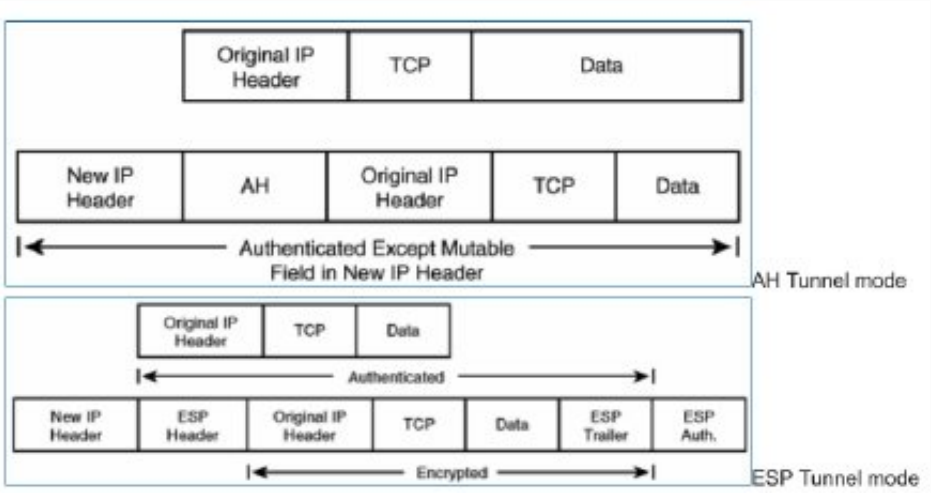
IPSec可以保证入口对入口通信安全，在此机制下，分组通信的安全性由单个节点提供给多台机器；同时，端到端分组通信安全，由作为端点的计算机完成安全操作。

IPSec 协议工作在 **OSI** 模型的第三层，使其在单独使用时适于保护基于 **TCP** 或 **UDP** 的协议。与传输层或更高层的协议相比：IPsec协议必须处理可靠性和分片的问题；它的复杂性更高。

*隧道模式和传输模式是**IPSec**最主要的两种运行模式。*

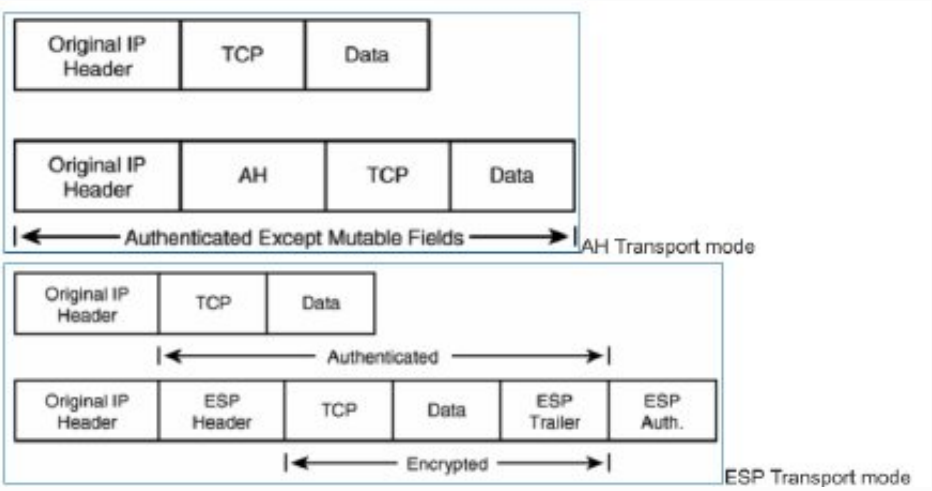
隧道模式

隧道模式保护所有 IP 数据并封装新的 IP 头部，不使用原始 IP 头部进行路由。在 IPSec 头部前加入新的 IP 头部，源目为 IPSec peer 地址。并允许 RFC 1918 规定的地址参与 VPN 穿越互联网。



传输模式

传输模式保护原始 IP 头部后面的数据，在原始 IP 头和 payload 间插入 IPSec 头部（ESP 或 AH）。典型应用为端到端的会话，并且要求原始 IP 头部全局可路由。

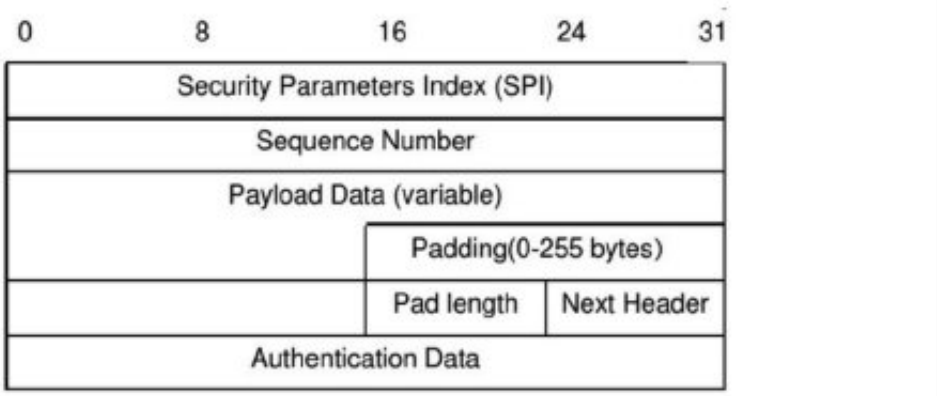


与隧道模式不同，当 **IPSec** 工作在传输模式时，新的 IP 头并不会被生成，而是采用原来的 IP 头，保护的也仅仅是真正传输的数据，而不是整个IP报文。在处理方法上，原 IP 报文会先被解开，再在数据前面加上新的 ESP 或 AH 协议头，最后再装回原来的 IP 头。

ESP报文

封装安全载荷协议（**ESP**），**IPSec** 所支持的两类协议中的一种。该协议能够在数据的传输过程中对数据进行完整性度量，来源认证以及加密，也可防止回放攻击。**ESP** 包大致结构可见上图：传输模式——ESP传输模式。

ESP 的数据封装格式如下：



ESP报文的装包与拆包

装包

1. 在原IP报文末尾添加 **ESP** 尾部信息。
2. 将原IP报文以及第1步得到的 **ESP** 尾部作为一个整体进行加密。
3. 为第2步得到的加密数据添加 **ESP** 头部。
4. 对第三步得到的加密数据与 **ESP** 头做摘要，得到一个完整性度量值，附在报文尾部。
5. 得到原本的IP头。
6. 发送 **ESP** 报文了。

拆包

1. 查看 **ESP** 头， 通过里面的SPI决定数据报文所对应的 SA。
2. 对加密数据与 **ESP** 头做摘要，与附在末尾的完整性度量值做对比，判断完整性。
3. 检查 Seq 里的顺序号，保证最新数据。
4. 根据SA所提供的加密算法和密钥，解密被加密过的数据——加密数据与 **ESP** 头。
5. 得到原 IP 报文与 **ESP** 尾部。
6. 找出填充字段的长度，得到原来的 IP 报文。
7. 转让到一个高一级的协议层（**UDP** 或 **ICP**），对这个包进行处理。

参考

"喝水不忘挖井人"，在此感谢为我提供思路的参考：

- 传输模式下ESP的装包与拆包过程
- **TCP-IP** 详解：ESP(IPSec Encapsulating Security Payload)
- 在**IPSec**传输模式下ESP报文装包和拆包过程
- 传输模式下ESP的装包和拆包过程
- **Psec**维基百科
- WEB安全——**IPsec**传输模式下ESP报文的装包与拆包过程
- **IPSec**详细介绍