flexedge版本IPSEC

# 一、基本学习资料

1. [IPSec VPN基本原理](http://www.h3c.com/cn/d_201005/675214_97665_0.htm)
2. [IPSec方案部署](http://www.h3c.com/cn/d_201007/683256_97665_0.htm)
3. [IPSec穿越NAT](http://www.h3c.com.cn/MiniSite/Technology_Circle/Technology_Column/ICG/ICG_Technology/201006/677319_97665_0.htm)
4. [IPSec拆包及封包流程](https://www.cnblogs.com/yanhewu/p/7782871.html)（重要）
5. [IPSec NAT-T技术实现nat穿越](https://www.cnblogs.com/hugetong/p/11482883.html)
6. [IPsec在NAT环境中应用](https://blog.csdn.net/mazhen12306/article/details/77427334)
7. [华为ipsec配置介绍](https://support.huawei.com/enterprise/zh/doc/EDOC1000177966/e4f5b42d)

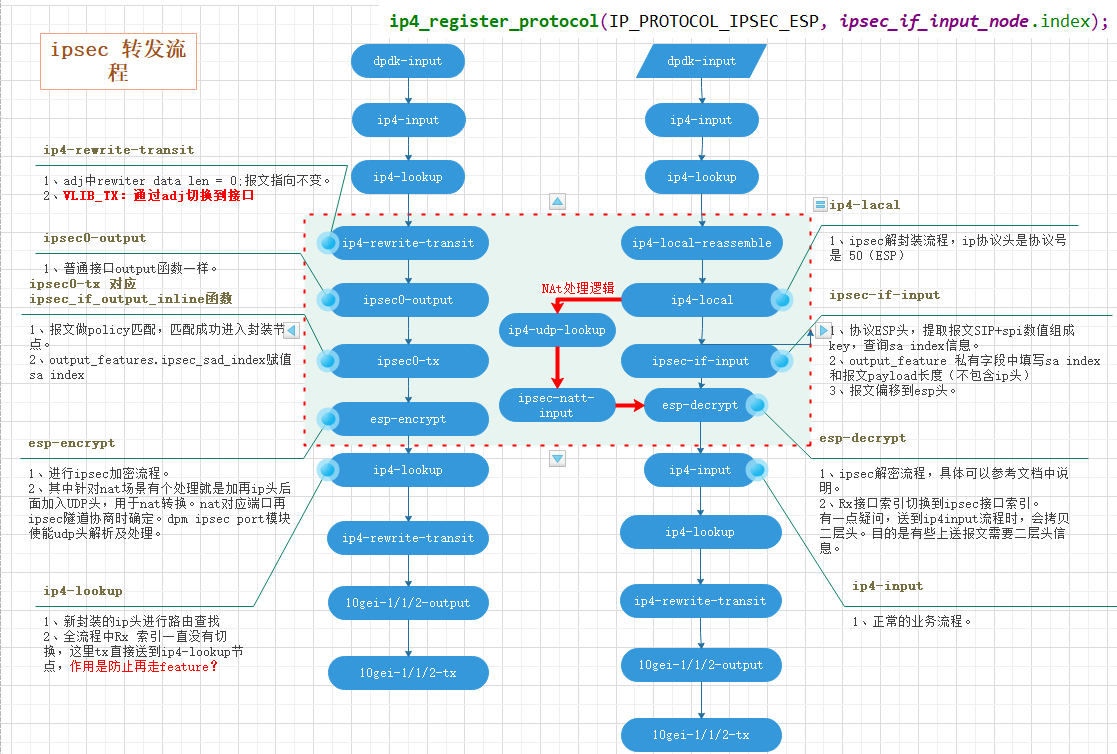
[文档：ipsec 隧道报文转发流程.note链接：](http://note.youdao.com/noteshare?id=adad69abe9a718e75b79371ad6948357&sub=DB9C1084D3B34A1BA2A62EAE2142359B)

Flexedge 版本支持加密算法ASE和国密算法。

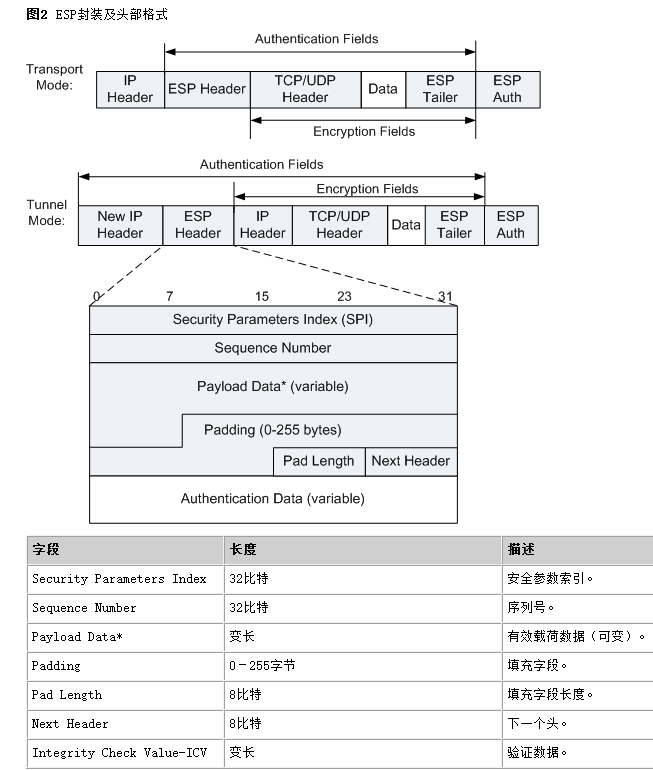
报文封装模式只支持隧道模式封装。

IPSec隧道建立大部分都是野蛮模式（3次交互），主动模式（不清楚）测试应该没有测试过。

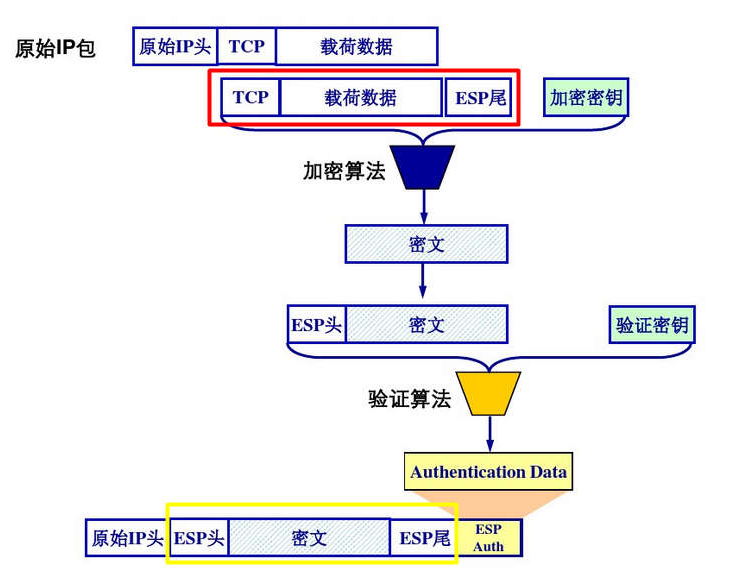




# IPsec拆包及封包流程



## IPsec封包流程

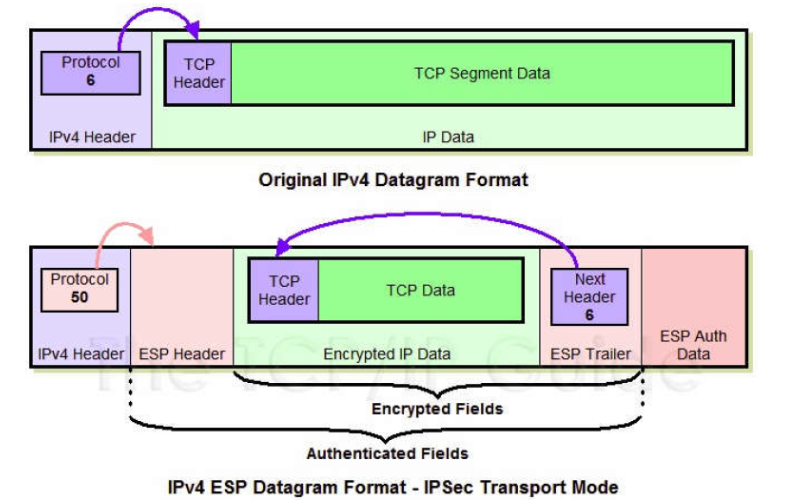


1. 在原IP报文中找到TCP报文部分，在其后添加相应的ESP trailer信息。

ESP trailer 包含三部分：Padding，Pad length 和 Next header。Padding 即使用块加密时，最后一个数据块长度不足时所做的填充。Pad length 指填充的长度，方便拆包时找到用来填充的数据段。Next header 标明被封装的原报文的协议类型，例如 6 = TCP。

1. 将原 TCP 报文和第1步得到的 ESP trailer 作为一个整体进行加密封装。具体的加密算法和密钥由SA给出。
2. 为第2步得到的密文添加 ESP 头。ESP 头由 SPI (Security Parameter Index) 和 Seq # 两部分组成。密文和 ESP头合起来称为"enchilada"，构成认证部分。
3. 附加完整性度量结果（ICV）。对第3步生成的"enchilada"认证部分做摘要（ESP Authentication Data），得到一个32位整数倍的 ICV，附在"enchilada"之后。ICV 生成算法和验证密钥由 SA 给出。
4. 将原始的 IP 报文头中的协议号改为50（代表 ESP），然后将 IP 报文头加到第4步的结果之前构成 IPsec 报文。

## IPsec拆包流程



1. 接收方收到 IP 报文后，发现协议类型是50，标明这是一个 ESP 包。首先查看 ESP 头，通过安全参数索引号 SPI 决定数据报文所对应的 SA，获得对应的模式（隧道或传输模式）以及安全规范。
2. 根据 SA 指定的摘要算法和验证密钥计算"enchilada"的摘要值，与附在 IP 报文最后的 ICV 进行对比，二者相同则数据完整性未被破坏。
3. 检查 ESP 头中的 Seq # 里的序列号，保证数据是新的，避免重放攻击。
4. 根据 SA 所指定的加密算法和密钥，解密密文段，得到原来的 TCP 报文和 ESP trailer。
5. 根据 ESP trailer 的填充长度信息，找出填充字段的长度，删除填充字段得到原来的 TCP 报文。
6. 根据 TCP 报文头信息将报文交付给传输层