---------------------------------------------------------------------

# 文档声明

## 合规性提示

本文档仅用于SSL VPN技术原理及应用场景的知识科普，不涉及任何翻墙工具的推荐、使用指导或技术破解内容。根据中国法律法规，未经许可私自使用VPN访问境外网络属于违法行为，相关使用需严格遵守国家网络安全管理规定及企业合规要求。

## 版权与使用说明

本文档所有内容（包括技术原理、分类说明、应用场景等）均为作者原创整理，仅供个人学习、研究参考使用，禁止用于任何商业用途（如付费课程、商业出版物、盈利性内容分发等），禁止以任何形式（包括完整转载、节选、截图、二次编辑后转发等）在其他平台传播。任何获取、使用本文档的用户，均需完整保留作者信息及本声明内容，不得抹去或修改原创标识。

## 内容免责

本文档内容仅为技术知识梳理，不构成专业指导建议。因引用本文档内容导致的任何直接或间接后果（包括但不限于信息误差、合规风险、第三方投诉等），作者不承担法律责任。文档中提及的技术方案（如SSL VPN协议、实现流程）仅作原理说明，具体使用需结合当地法律法规及企业内部规范。

---------------------------------------------------------------------

# IPsec

## 0 序言

IPsec是一个用于保护IP层通信安全的协议，为IP数据包提供机密性、完整性、数据发送方身份认证以及抗重放攻击等能力。其工作过程分为：安全关联（SA）建立、数据传输保护、安全关联的维护与销毁。

安全关联（SA）是IPsec协议的基础，是通信双方协商的安全算法。SA是通信单向的，即源通信1需要向源通信2建立SA，反过来源通信2也要向源通信1建立SA，在一个SA中，双方需要协商相同的安全算法，在不同的SA之间没有必然的相关性，即两个SA可以使用不同的安全算法。

互联网密钥交换（IKE）协议是IPsec的重要组成部分，它利用公钥技术，帮助通信双方共享一个对称加密密钥。

## 1 阶段1——建立IKE SA

本阶段的目标是认证通信双方的身份、协商IKE的安全策略并生成共享密钥。

本阶段支持两种模式：详细模式（Main Mode）和简单模式（Aggressive Mode）【不要介意作者的翻译水平】。详细模式将身份数据进行加密，安全性高，适合需要向公网以及传输设备隐藏身份的通信。简单模式则对敏感性不高的数据（比如内网IP地址、身份信息等）不加密，适合低安全要求且需要快速的远程访问场景。

### 1.1 Main Mode的消息交互

1.A向B发送自己支持的安全策略，包括IKE SA协商过程的加密算法、认证短发、DH密钥交换的参数组、SA生命周期、密钥派生算法等内容。

2.B根据A发送的策略与自己支持的策略对比，选择双方均支持的策略，发送给A。

3.A生成一个临时私钥a，并根据B返回确认的DH参数组计算公钥，将公钥发送给B。

4.B生成一个临时私钥b，根据确认的DH参数组计算公钥，将公钥发送给A。

【双方收到对方的公钥后，立刻根据对方公钥得出共享密钥（具体的DH协商共享密钥可以参见IPsec VPN）】

5.双方进行身份认证（**使用主密钥派生的密钥加密该消息**）。【使用预共享密钥完成认证可参考IPsec VPN】

使用数字证书完成认证的具体方法：

前提是双方均需要有由CA机构颁发的证书。证书内容至少包括：证书有效期+证书序列号等基本的证书信息、公钥+持有者身份、签名算法及其顺序、CA机构使用具有公信力的公私钥中的公钥对前面的信息进行的签名。只需要使用CA的公钥对签名进行验证运算（验证时需要考虑签名算法）就能验证身份。

签名算法可以采用一个哈希函数（不带密钥）或者哈希校验（带密钥，可以选择为要签名者持有的公钥进行的派生，并在签名算法中标注派生算法）将长信息进行压缩，最后对这个压缩值进行签名。

数字签名能够抵御中间人攻击的核心在于任何除了CA机构之外的人想要从CA的公钥与算法中获取其对应的私钥是几乎不可能的。中间人最想干的就是将双方认证过的公钥改成自己的公钥，以便解密信息，但这样就必须知道CA签名的私钥进行签名运算，否则他的存在将会被通信双方察觉。

### 1.2 Aggressive Mode的消息交互

1.A向B发送自己支持的策略、公钥、身份等信息。

2.B向A发送选定的策略、公钥、身份等信息，并生成AUTH（基于SKEYID\_a的哈希或签名）。

3.A验证B的身份并发送自己的AUTH，让B完成验证。

【双方收到对方的公钥后，立刻根据对方公钥得出共享密钥，并派生IKE会话密钥】

SKEYID\_a = Hash(共享密钥||随机数1||随机数2||身份1||身份2)【||表示二进制填充拼接，填充规则由Hash决定】

PSK 认证：AUTH = HMAC-SHA256（SKEYID\_a, 消息内容1||消息内容2）

签名认证：AUTH = Sign(Hash(SKEYID\_a, 消息内容1||消息内容2))

### 1.3 Main Mode与Aggressive Mode对比

Main Mode需要6个数据包（身份认证要两个），而Aggressive Mode却只要3个数据包。

Main Mode使用的身份认证能够抵抗中间人攻击，而Aggressive Mode使用的身份认证能够被中间介入（因为无法确认设备的身份信息究竟是否是期望的而不是中间人的，除非将Aggressive Mode的身份认证改成CA数字证书认证）。

## 2 阶段2——建立IPsec SA

在阶段1的IKE SA通道下协商IPsec的安全策略并派生会话密钥。

1.A生成随机数用于派生会话密钥，并向B发送IPsec策略提议与这个随机数。

2.B选择合适的策略，生成随机数用于派生会话密钥，并将这些信息发给A。

【这两次会话是使用IKE SA的会话密钥加密过的，Main Mode模式早在身份认证阶段就开始使用IKE会话密钥加密了】

## 3 阶段3——数据传输

IPsec通过AH（Authentication Header）或者ESP（Encapsulating Security Payload）实现数据保护。

AH通过设置序列号和哈希确保消息的完整性和抗重放攻击性。AH将IP数据包与AH序列号进行带密钥的哈希运算值置于数据包中。一般来说，AH应当对加密的IP数据包进行认证。

ESP先使用加密算法加密明文（根据模式选择是否加密IP头部），再生成ESP头部（含序列号）和ESP尾部（含加密算法参数），后对这个ESP数据报进行哈希值计算，生成认证数据。最后将ESP数据包封装在IP头后（传输模式）或者新的IP头内（隧道模式）。【传输模式仅保护数据而不保护IP头，适用于主机到主机的通信；隧道模式将整个IP数据包加密，添加新的IP头部，比如VPN网关，适用于网关到网关和网关到主机的通信】

## 4 SA的维护与销毁

Psec SA 有生命周期（时间或数据量阈值，如 1 小时或 1GB），到期前 IKE 会自动重新协商（通过阶段 2 的快速模式），生成新的 IPsec SA（无缝切换，不中断通信）；过期的 SA 则被销毁，释放资源。

**本文章归属 github 用户 WhatTheFuck-cyber**