URPF

URPF（Unicast Reverse Path Forwarding）是单播逆向路径转发的简称，其主要功能是防止基于源 IP 地址欺骗的网络攻击行为,防止 ddos 攻击。

（1）工作模式

在复杂的网络环境中应用 URPF 时，会遇到路由不对称的情况，即对端设备记录的路由路径不一样，此时使能 URPF 的设备可能丢弃合法报文，造成设备不能正确转发。为了解决以上复杂网络中应用 URPF 的问题，设备实现了 URPF 的两种工作模式：

1 严格模式（防止源欺骗攻击）

严格模式下，设备不仅要求报文源地址在 FIB 表中存在相应表项，还要求接口匹配才能通过 URPF 检查。建议在路由对称的环境下使用 URPF 严格模式，例如两个网络边界设备之间只有一条路径的话，这时，使用严格模式能够最大限度的保证网络的安全性。

应用场景：防止攻击者伪造合法用户的 IP 地址，对某台服务器或主机进行攻击。

2 松散模式（防止 ddos 攻击）

松散模式下，设备不检查接口是否匹配，只要 FIB 表中存在该报文源地址的路由，报文就可以通过。建议在不能保证路由对称的环境下使用 URPF 的松散模式，例如两个网络边界设备之间如果有多条路径连接的话，路由的对称性就不能保证，在这种情况下，URPF 的松散模式也可以保证较强的安全性。

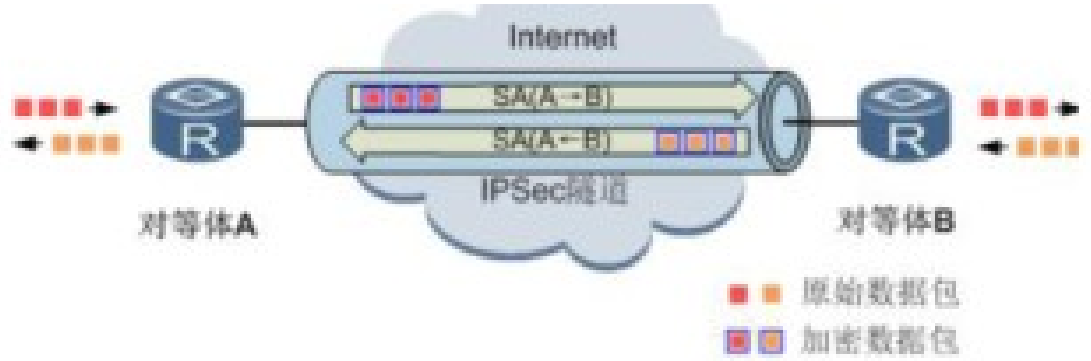
IPSec

IPSec（Internet Protocol Security）是 IETF（Internet Engineering Task Force）制定的一组开放的网络安全协议，在 IP 层通过数据来源认证、数据加密、数据完整性和抗重放功能来保证通信双方

Internet 上传输数据的安全性。
1 数据来源认证：接收方认证发送方身份是否合法。
2 数据加密：发送方对数据进行加密，以密文的形式在 Internet 上传送，接收方对接收的加密数据进行解密后处理或直接转发。
3 数据完整性：接收方对接收的数据进行认证，以判定报文是否被篡改。
4 抗重放：接收方会拒绝旧的或重复的数据包，防止恶意用户通过重复发送捕获到的数据包所进行的攻击。

在 Internet 的传输中，绝大部分数据的内容都是明文传输的，这样就会存在很多潜在的危险，比如：密码、银行帐户的信息被窃取、篡改，用户的身份被冒充，遭受网络恶意攻击等。网络中部署 IPSec 后，可对传输的数据进行保护处理，降低信息泄漏的风险。
（1）IPSec 基本概念：
1 认证头协议 AH（Authentication Header）、
2 .封装安全载荷协议 ESP（Encapsulating Security Payload）、
3. 因特网密钥交换协议 IKE（Internet Key Exchange），用于保护主机与主机之间、主机与网关之间、网关与网关之间的一个或多个数据流。
4 IPSec 对等体：IPSec 用于在协商发起方和响应方这两个端点之间提供安全的 IP 通信，通信的两个端点被称为 IPSec 对等体。其中，端点可以是网关路由器，也可以是主机。
5 IPSec 隧道：IPSec 为对等体间建立 IPSec 隧道来提供对数据流的安全保护。一对 IPSec 对等体间可以存在多条 IPSec 隧道，针对不同的数据流各选择一条隧道对其进行保护，例如有的数据流只需要认证、有的需要认证和加密。
6 安全联盟：用 IPSec 保护数据之前，必须先建立安全联盟 SA（Security Association）。SA 是出于安全目的而创建的一个单向逻辑连接，是通信的对等体间对某些要素的约定，例如对等体间使用何种安全议、需要保护的数据流特征、对等体间传输的数据的封装模

式、用于数据安全转换和传输的密钥以及 SA 的生存周期等。对等体间需要通过手工配置或 IKE 协议协商匹配的参数才能建立起安全联盟。所有经过同一 SA 的数据流会得到相同的安全服务，如 AH 或 ESP。如果对同一个数据流同时使用 AH 和 ESP 服务，则针对每一种协议都会构建一个单独的 SA。对等体之间的双向通信需要建立一对 SA，这一对 SA 对应于一条 IPSec 隧道。IPSec 建立的 SA 和隧道如图 1 所示，数据从对等体 A 发送到对等体 B 时，对等体 A 对原始数据包进行加密，加密数据包在 IPSec 隧道中传输，到达对等体 B 后，对等体 B 对加密数据包进行解密，还原成原始数据包。数据从对等体 B 发送到对等体 A 时，处理也类似，但所在的 SA 不同。



备注:

1 AH 和 ESP 这两个安全协议用于提供安全服务，IKE 协议用于密钥交换。

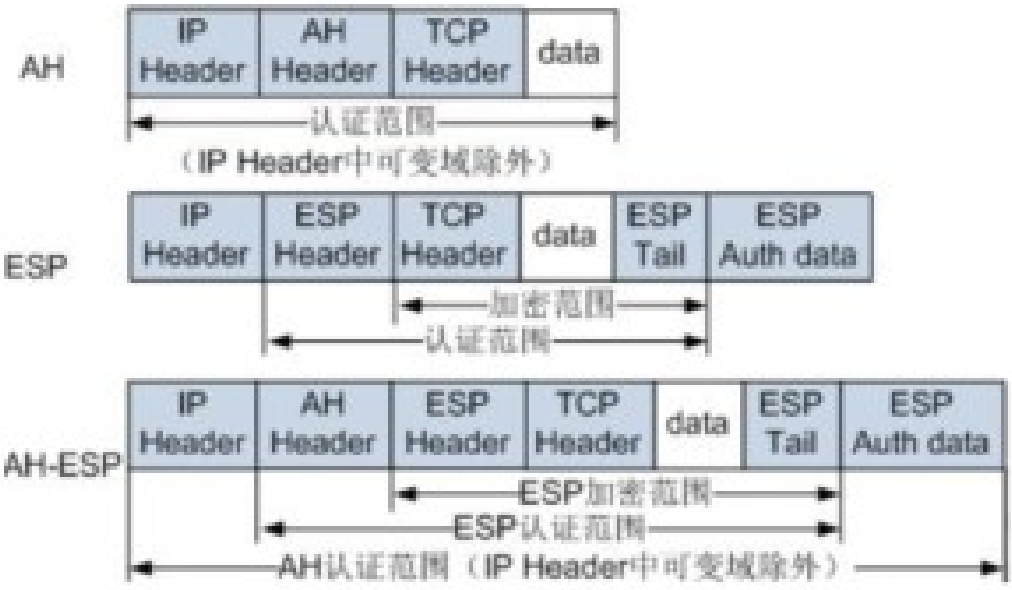
2 IPSec 对数据的加密是以数据包为单位。发送方对要保护的数据包进行加密封装，在 Internet 上传输，接收方采用相同的参数对报文认证、解封装，以得到原始数据。

3 IPSec 通过在 IPSec 对等体间建立双向安全联盟，形成一个安全互通的 IPSec 隧道，来实现 Internet 上数据的安全传输。

SA 由一个三元组来唯一标识，这个三元组包括安全参数索引 SPI（SecurityParameter Index）、目的 IP 地址（SA 的终端地址）和使用的安全协议。

有以下两种方式建立 SA：
1 手工方式：SA 所需的全部信息都必须手工配置。
2 IKE 动态协商方式：由 IKE 协议完成密钥的自动协商，实现动态协商来创建和维护 SA。
手工方式适用于对等体设备数量较少时，或是在小型网络中。
对于中大型网络，推荐使用 IKE 协商建立 SA。

（2）安全协议
1 认证头协议 AH：提供数据来源认证、数据完整性校验和报文抗重放功能。
AH 的工作原理是在每一个数据包的标准 IP 报头后面添加一个 AH 报头(AH Header)，如图 3 所示。AH 对数据包和认证密钥进行 Hash 计算，接收方收到带有计算结果的数据包后，执行同样的 Hash 计算并与原计算结果比较，传输过程中对数据的任何更改将使计算结果无效，这样就提供了数据来源认证和数据完整性校验。



2 封装安全载荷协议 ESP：除提供 AH 的功能之外，还提供对有效载荷的加密功能。ESP 协议允许对报文同时进行加密和认证，或

只加密，或只认证。ESP 的工作原理是在每一个数据包的标准 IP 报头后面添加一个 ESP 报头(ESP Header)，并在数据包后面追加一个 ESP 尾（ESP Tail 和 ESP Authdata），如图 3 所示。与 AH 不同的是，ESP 尾中 ESP Authdata 用于对数据提供来源认证和完整性校验，并且 ESP 将数据中的有效载荷进行加密后再封装到数据包中，以保证数据的机密性，但 ESP 没有对 IP 头的内容进行保护。

ESP 支持的认证算法与 AH 支持的认证算法相同，它支持的加密算法有 DES（Data Encryption Standard）、3DES（Triple DES）、AES（Advanced EncryptionStandard）、SM1。前三个加密算法的安全性由低到高依次排列，其计算速度随安全性的提高而减慢。

AH 和 ESP 报头共同包含的信息分别为 32 比特数值的 SPI 和序列号。SPI 用于在接收端识别数据流与 SA 的绑定关系。序列号在通信过程中维持单向递增，可以在对等体间提供数据抗重放服务，例如，当接收方收到报文的序列号与已经解封装过的报文序列号相同或序列号较小时，会将该报文丢弃掉。

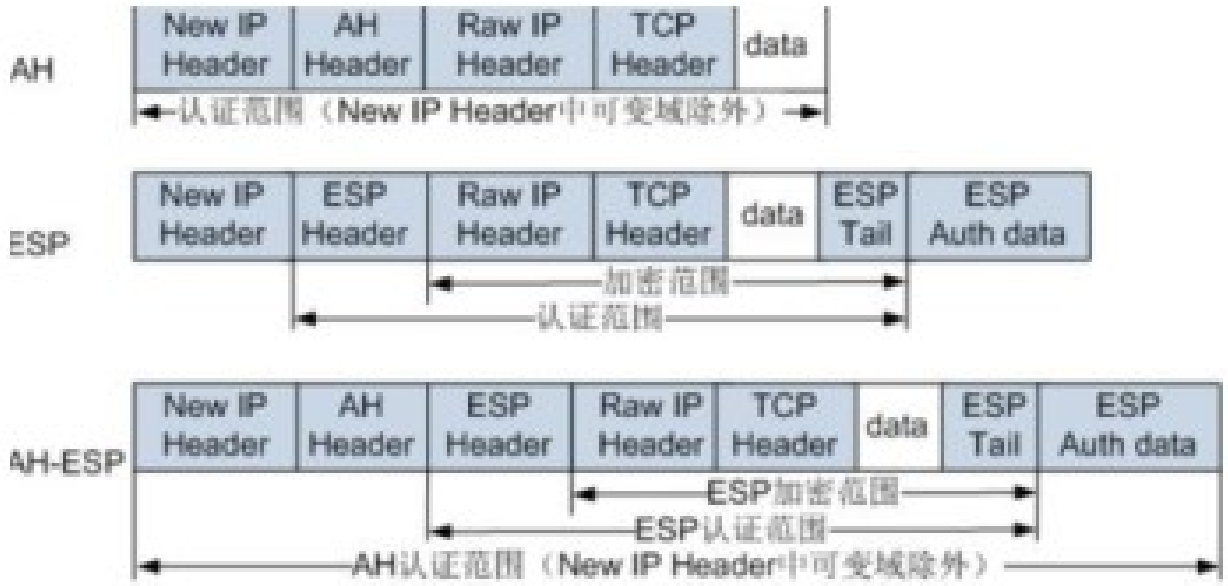
AH 能保护通信免受篡改，但不能防止报文被非法获取，适合用于传输非机密数据。ESP 虽然提供的认证服务不如 AH，但它还可以对有效载荷进行加密。
用户可以根据实际安全需求选择使用其中的一种或同时使用这两种协议。在同时使用 AH 和 ESP 的情况下，IPSec 加封装时，设备先对报文进行 ESP 封装，再进行 AH 封装；IPSec 解封装时，设备先对报文进行 AH 解封装，再进行 ESP 解封装。

（3）数据的封装模式
数据的封装是指将 AH 或 ESP 相关的字段插入到原始 IP 报文中，以实现对报文的认证和加密，数据的封装模式有隧道模式和传输模

式两种。

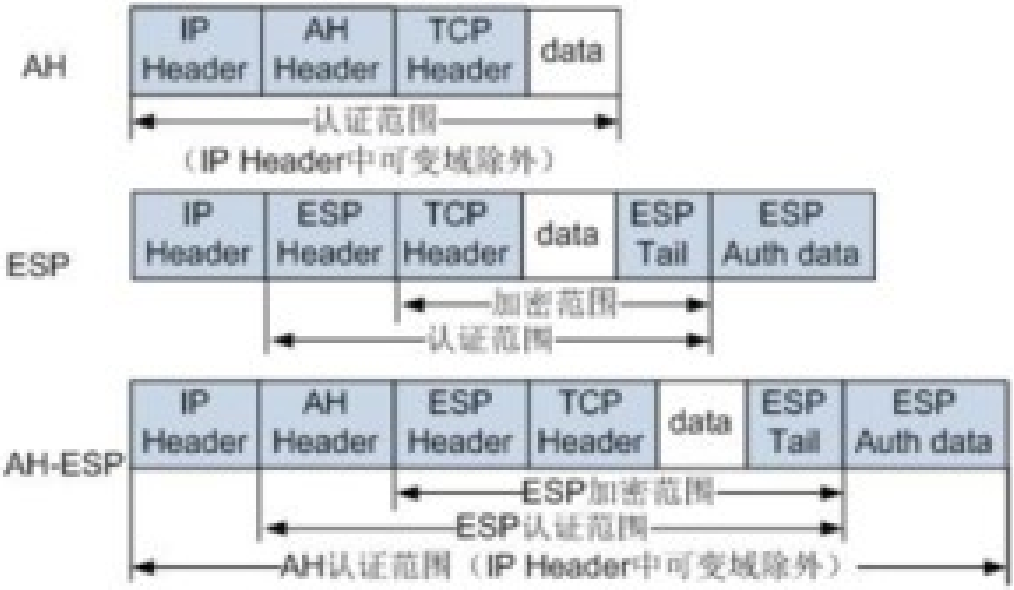
1 隧道（Tunnel）模式：

在隧道模式下，AH 报头或 ESP 报头插在原始 IP 头之前，另外生成一个新 IP 头（新 IP 头为对等体的 IP 地址）放到 AH 报头或 ESP 报头之前。隧道模式在两台主机端到端连接的情况下，隐藏了内网主机的 IP 地址，保护整个原始数据包的安全。以 TCP 为例，如图 2 所示。



2 传输（Transport）模式

在传输模式下，AH 报头或 ESP 报头被插入到 IP 头之后但在传输层协议之前。传输模式保护原始数据包的有效负载。



隧道模式适于转发设备对待保护流量进行封装处理的场景，建议应用于两个安全网关之间的通讯。
传输模式适于主机到主机、主机到网关对待保护流量进行封装处理的场景。
从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据包进行认证和加密，并且可以使用对等体的 IP 地址来隐藏客户机的 IP 地址。从性能来讲，因为隧道模式有一个额外的 IP 头，所以它将比传输模式占用更多带